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 SKELETON ARGUMENT

For hearing commencing: Tuesday 26 July 2016

Amended with Bundle References

Suggested pre-reading:

- List of issues [CORE/A10]

- Schedule of agreed and assumed facts [CORE/C]

- Witness statements of Smith, Graham Wood, Wilson Palow [CORE/B1] and the GCHQ, SIS and Security Service witnesses [CORE/B2]

A. Introduction

BPD and BCD

1. This claim is about the acquisition, use, retention, disclosure, storage and deletion of:

   a) Bulk Personal Datasets ("BPDs"); and

   b) Bulk Communications Data ("BCD") obtained under section 94 of the Telecommunications Act 1984 ("TA") [A1/1]

   by GCHQ, SIS and the Security Service (together referred to below as "the Agencies").

2. The key facts are agreed, save that sharing of section 94 data with HMRC and the NCA is neither confirmed nor denied, and is to be assumed for the purposes of the preliminary hearing.

3. BPD and BCD are intrusive and comprehensive. GCHQ "*keep the entirety of all the communications data that comes into the building…*" (IOCCO visit 15 May 2013 [3/520]). Current BCD collection includes location information and call data for everyone's mobile telephones in the UK for 1 year (Amended Security Service Witness Statement, §§ 25 and 130 [CORE/B2]).

4. Current BPDs held by the Agencies include:

   a) "*bulk travel data*";

   b) "*bulk untargeted communications metadata*";

   c) "*anonymised records of financial transactions*" (Hannigan Report §26, 27, 30 [3/569-70]);

   d) bulk databases obtained by computer hacking (GCHQ Closed Handling arrangements, para. 4.2 [4/A/139]); and

   e) "*internet network management data and logs… includ*[ing] *data of UK persons*" (Response to Supplemental RFI §77 [CORE/A9/21]).

5. Examples of "*bulk travel data*" might include:

   i) immigration records;

   ii) airline booking records;

   iii) hotel reservations;

   iv) automatic number plate recognition data and roadside camera photos;

   v) London Oyster card and contactless credit card travel records;

   vi) laptop computer and mobile telephone wifi connection logs; and

   vii) mobile telephone location data from cellular masts.

6. The Security Service only classifies such information as of "*MEDIUM… actual intrusion level*" even where it identifies a detailed picture of the personal activities of many people of no real intelligence interest:

   > "*Dataset: Travel Data…*
   >
   > > *Commentary: Results of a query would identify the movements of the individuals subject to the query. Due to limited intelligence it is common for queries to be conducted and return data on people of no intelligence interest.*
   > >
   > > *Intrusion is minimised through limiting access and ensuring that all searches are specific and subject to audit. Handling caveats are also imposed to limit risk" (RFI 15)* [3/180].

7. Multiple datasets are joined together to enable profiling of the whole population. The GCHQ witness describes "*very powerful, and very fast, data fusion*" (§9 [CORE/B2]). It

is common ground that such conduct increases the intrusion into privacy considerably:

> *"While each of these datasets in themselves may be innocuous intelligence value is added in the interaction between multiple datasets. One consequences of this is that intrusion into privacy can increase"* (Closed Response, §4 [CORE/A6/2]).

8. The Agencies often claim that communications data and datasets excluding content are not particularly intrusive. That suggestion is wrong. Such data, using profiling techniques, makes it possible *"to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity"* (*Digital Rights Ireland* [A3/62] per AG Cruz Villalón at §72-74). In *Watson & Others* [A3/63], Advocate General Saugmandsgaard Øe agreed at §259:

> *"I would emphasise that the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications … . … 'metadata' facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not."*

The parties

9. Privacy International is a charity. It seeks to ensure that surveillance and the collection and use of data is carried out within the law, providing protection for the right to privacy.

10. The Secretary of State for Foreign and Commonwealth Affairs is the minister responsible for oversight of the Government Communication Headquarters ("GCHQ") and the Secret Intelligence Service ("SIS"). The Secretary of State for the Home Department is the minister responsible for the Security Service.

Issues

11. The issues are agreed. In summary:

    a) Issue 1: Section 94 TA under domestic law: Is it lawful as a matter of domestic law to use section 94 TA to obtain BCD?

    b) Issue 2: Is section 94 TA regime in accordance with the law? This issue is to be considered in three time periods. First, prior to the avowal of the use of section 94 to obtain BCD. Secondly, from avowal to the date of hearing. Thirdly, as at the date of hearing.

    c) Issue 3: Is the BPD regime in accordance with the law? This issue is to be considered in four time periods. First, prior to the avowal of the holding of BPDs. Secondly, from avowal to the publication of the BPD handling arrangements. Thirdly, from publication to the date of the hearing. Finally, as at the date of hearing.

    d) Issue 4: Is the section 94 regime and the BPD regime proportionate?

12. The EU law issues have been adjourned until November 2016, pending judgment in the Court of Justice in Case C-698/15 *Watson & Others* [A3/63].

Disclosure and Schedule

13. Disclosure of key materials has arrived very late and piecemeal. The last tranche of disclosure arrived on the evening of Friday 15 July. It became apparent that this material had been incorrectly redacted. Substantial important material, previously disclosed in open, had been re-redacted. The Claimant was only able to identify this problem by carrying out a laborious manual comparison. Corrected documents were served yesterday afternoon, 19 July. The Claimant is continuing to analyse the disclosure and may need to supplement its submissions in due course.

14. This skeleton is accompanied by a Schedule summarising the Claimant's case by reference to the different time periods set out above.

B. Section 94 of the Telecommunications Act 1984

15. Section 94 TA [A1/1] permits the Secretary of State to give national security directions to OFCOM and to providers of public electronic communications networks ("PECNs").

16. Section 94 (as amended) provides:

> *(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*
>
> *(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.*
>
> *(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.*
>
> *(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.*
>
> *(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.*
>
> *(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.*
>
> *(6) The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purpose of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.*
>
> *(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.*
>
> *(8) This section applies to OFCOM and to providers of public electronic communications networks.*

17. Only two section 94 directions have ever been made public. One concerns international dialling codes. Another requires O2 (UK) Limited to create a national security sub-committee of its board, and relieves the sub-committee of any obligation to report to the main board. It is assumed that this direction was the precursor to the service of a section 94 BCD direction in 2005.

18. In the summer of 2015, a respected national security journalist reported that section 94 had been used to require telecommunications companies to provide BCD to the Agencies outside the protections of the Regulation of Investigatory Powers Act 2000 ("RIPA") regime (Gordon Corera, *Intercept: The Secret History of Computers and Spies* (2015) p. 332).

19. The use of section 94 for this purpose was eventually avowed in November 2015 on the publication of the draft Investigatory Powers Bill (Response to RFI, §4 [CORE/A4/3]). HM Government confirmed that section 94 has been used to require telecommunications companies to provide communications data in bulk to GCHQ and the Security Service.

20. Since 3 June 2016, on the service of evidence by the Respondents (with amended versions served on 8 and 11 July 2016), it has become clear that:

    a) GCHQ has used section 94 directions for collecting BCD since March 1998 (Amended GCHQ Witness Statement, § 117 [CORE/B2]).

    b) GCHQ combines data acquired under section 94 directions into the databases holding communications data obtained under section 8(4) RIPA warrants (Amended GCHQ Witness Statement, § 128 [CORE/B2]) (Amended RFI Response, § 81 [CORE/A9/22-23]).

    c) The first directions made at the request of the Security Service were issued in July 2005 (Amended Security Service Witness Statement, § 109 [CORE/B2]).

    d) BCD may include locational information (Amended Security Service Witness Statement, § 25 [CORE/B2]).

    e) The Security Service generally retains BCD for one year (Security Service Closed section 94 Arrangements, §3.18 [4/B/173] and Amended Security Service Witness Statement, § 130 [CORE/B2]).

    f) Since 2012, GCHQ has also obtained Internet communications data (Amended GCHQ Witness Statement, § 122 [CORE/B2]). The nature of that data has not been explained. That data was collected for the purpose of the "*cyber defence*" of the UK, but has since been re-used for other purposes (Amended RFI response, § 77 [CORE/A9/21]).

21. As to the oversight regime:

    a) There is not, and has never been, any statutory oversight regime covering section 94.

    b) Initial consultations with Sir Swinton Thomas in 2004 were on the basis that the acquisition of the communications data by *either* section 94 TA or Chapter 2 of Part I of RIPA was lawful (Sir Stanley Burton, *Report of the Interception of*

Communications Commissioner: Review of directions given under section 94 of the Telecommunications Act (1984), July 2016 ("the Burnton Report"), § 8.23 [A4/82]). However, that legal analysis was manifestly inadequate (see the Burnton Report, §§ 8.25-26):

> *'… the Home Office advice did not provide an analysis as to why the interference at the acquisition stage (using section 94 directions) was deemed to be in accordance with Article 8 of ECHR. The historic correspondence does not recognise that bulk communications data is personal data or refer to the Council of Europe's 2002 "Guidelines on human rights and the fight against terrorism" … . Suffice to say that our review of this historic correspondence, taking into account the case law and guidance that was available at the time, shows its consideration of the legal issues to have been incomplete. …'*

c) There has been only limited non-statutory oversight thereafter. The oversight of section 94 directions between 2004 and 2015 was summarised in the Burnton Report as follows (§ 2.5):

> '*This previous oversight (between 2006 and 2015) was limited because it was only concerned with the authorisations to access the communications data obtained pursuant to the directions. The oversight was not concerned with, for example, the giving of the section 94 directions by the Secretary of State (including the necessity and proportionality judgements by the agency or Secretary of State) or the arrangements for the retention, storage and destruction of the data.*'

d) The former Interception of Communications Commissioner's (Sir Anthony May) report from July 2015 [A4/81] explained the limited nature of the oversight to date in the following terms (§ 4.7, emphasis in original):

> *My office previously provided <u>limited</u> non-statutory oversight of the use made of one particular set of section 94 directions. This oversight was limited because it was only concerned with parts of c) above [i.e. safeguards]. My office was, and still is, prohibited from saying any more about this oversight as the Secretary of State is of the opinion that disclosure would be against the interests set out in section 94(5) of the Telecommunications Act.*

e) Even the fact of this oversight was kept secret until the publication of the July 2015 report.

22. The proposals for oversight developed as follows:

a) The Interception of Communications Commissioner agreed to provide non-statutory oversight from March 2015 onwards over the (a) necessity and proportionality of section 94 directions; (b) the use of section 94; and (c) the safeguards for the use of section 94. The Commissioner explained that this work would not be able to begin immediately: "*I will therefore require extra staff (and possibly technical facilities) to be able to carry out this oversight properly*" (IOCCO Report, March 2015, §10.4 [A4/78]).

b) In July 2015, the Commissioner indicated that oversight had not yet started, and would not begin until "*the last quarter of 2015*" (IOCCO Report, July 2015, § 4.3 [A4/81]). The Commissioner explained the serious problems

encountered to date in his non-statutory oversight function (ibid, § 4.4, emphasis in original):

> *'There are, however, some considerable challenges in this regard. The challenges stem from the fact that the directions are secret as followed for by statute, can be given by* any *Secretary of State and do not automatically expire after a certain period. There does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State. My office is therefore not yet in a position to be able to say confidently that we have been notified of all directions.'*

23. The first serious attempt at oversight only commenced in recent months. The oversight regime continues to face (*inter alia*) the following difficulties:

a) There is no statutory provision for review of section 94 directions;

b) Section 94 directions do not expire (Amended GCHQ Witness Statement, § 144 [CORE/B2]);

c) There is no central register or reporting obligation to the Commissioner (cf. Recommendations 1 and 2 in the Burnton Report [A4/82]). The Burnton Report noted the difficulties cause by the fact that *'there is no code of practice or any written requirement for detailed record-keeping for public authorities or* [Public Electronic Communications Networks] *applicable to the operation of section 94 of the Telecommunications Act 1984'* (§ 5.4), and that it was challenging *'to piece together and determine historically what section 94 notices had been given, by whom and when, which ones had been modified and whether they were still extant or not'* (§ 5.10).

24. The Burnton Report made clear that, given the issues to be decided by the IPT in this case, the Commissioner's review did not seek to determine lawfulness (§ 3.3). The report nevertheless made a number of striking findings regarding the use of section 94 directions, including:

a) While the agencies submitted that *'the speed at which individual data requests (once authorised under Chapter 2 of Part 1 of RIPA) can be acquired from the communication service providers (CSPs), using the secure online workflow systems developed for this purposes, is not sufficient for them to meet their operational requirements'*, the Burnton Report concluded that this *'is arguably not the case when dealing with more routine requests which, within the agencies, form the majority'* (§ 8.31). It was also found that there was an urgent operational requirement to access the communications data only in *'a very small number of cases'* (§ 8.79). It is therefore unclear how these findings can be squared with the agencies' submissions regarding 'necessity'.

b) The GCHQ section 94 directions were *'very broad and provided a general description of communications data which was far wider than the requirement actually made of the PECN'* and the *'supporting documentation containing the specific data requirements has from time to time been modified to amend a data requirement (i.e. to extend or to cease certain data)'* (§ 8.42).

c) There are frequent errors when accessing BCD: '[b]*etween 1st January 2015 and the date of the completion of this report* [i.e. no later than 7th July 2016] *the Security Service reported 230 errors to us*' (§ 8.74).

d) The UK communication service providers have been uncomfortable about their role in providing data under section 94. For example, the Burnton Report cites PECNs' concerns that *'the section 94 provisions do not consider the multi-national nature of the PECN's business model or the fact that they have to operate in several legal jurisdictions'* (§ 6.7) and cites their *'concerns as to whether the bulk communications data they had disclosed had been shared with agencies in other jurisdictions. In one case a PECN had asked the agency to ensure that this did not happen'* (ibid).

25. The Burnton Report made the following nine recommendations:

a) *'Each public authority must keep a central record of all section 94 directions given by any Secretary of State on their behalf. …'*

b) *'Each time a section 94 direction is given by a Secretary of State it must be notified to the Commissioner by the public authority. In order to enable a reverse audit to be conducted, each time a section 94 direction is served on a PECN, the PECN should report the details of that direction to the Commissioner. '*

c) *'All section 94 directions for bulk communications data should indicate the specific communications data that is required to be disclosed by the PECN. When a requirement is amended (i.e. modified) a new direction should be given.'*

d) *'There should be a clear mandated application process for section 94 directions which sets out the requirements to be met. …'*

e) *'Where a PECN changes its company name or merges with another PECN, a new section 94 direction must be given to reflect the change.'*

f) *'There should be a clear written mandated process for the review, modification and cancellation of any section 94 directions. …'*

g) *'There should be a clear mandated process in place for the reporting of errors. That process should distinguish between errors that occur in the giving of, and conduct complying with, a section 94 direction and, where relevant, errors that occur when an agency accesses data that has been retained pursuant to a section 94 direction.'*

h) *'The public authorities should ensure they disclose or provide to IOCCO all such documents and information as the Commissioner may require in carrying out his inspection regime of section 94 directions. …'*

i) *'The public authorities with "other" section 94 directions should take steps to ensure that IOCCO is able to audit comprehensively the use made of any "other" section 94 directions. …'*

26. Reporting by the Independent Reviewer of Terrorism Legislation has also been critical. David Anderson QC in *A Question of Trust* (June 2015) [A4/80] said:

6.17 … s94… is very broad in nature and imposes no limit the kinds of direction that may be given. There is nothing in the public domain concerning the use of that power and the exercise of the s94 power is not subject to any oversight or external supervision…

13.31 … Obscure laws – and there are few more impenetrable than RIPA and its satellites – corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean. Thus… TA 1984 s94… are so baldly stated as to tell the citizen little about how they are liable to be used.

C. Bulk Personal Datasets

27. Until last year, the fact that the Agencies held BPD was kept secret (Response to RFI §1 [CORE/A4/2]).

28. On 12 March 2015, the Intelligence and Security Committee published its report "*Privacy and Security: A modern and accountable legal framework*" ("the ISC Report") [A4/79]. The ISC Report disclosed, for the first time, the existence of Bulk Personal Datasets:

> *'284. The publication of this Report is an important first step in bringing the Agencies 'out of the shadows'. It has set out in detail the full range of the Agencies' intrusive capabilities[1], as well as the internal policy arrangements that regulate their use. It has also, for the first time, avowed Bulk Personal Datasets as an Agency capability.'*

29. The ISC concluded: "*BBB. ... the time has come for much greater openness and transparency regarding the Agencies' work*".

30. The ISC gave the following explanation of Bulk Personal Datasets:

    a) Bulk Personal Datasets are "*large databases containing personal information about a wide range of people*" (p. 55).

    b) Bulk Personal Datasets are used to identify subjects of interest, establish links between individuals and groups and improve understanding of a target's behaviour and connections, and to verify information obtained from other sources (p. 55).

    c) The collection and search of Bulk Personal Datasets "*may be highly intrusive and impacts upon large numbers of people*" (p. 115).

    d) Bulk Personal Datasets are "*an increasingly important investigative tool*" (§153).

    e) Bulk Personal Datasets vary in size "*from hundreds to millions of records*" and may be "*linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or a ***) from one search query*" (§156).

31. The ISC reported adversely on the BPD legal regime:

    a) There has been minimal oversight and no clear public legal regime governing the use of Bulk Personal Datasets:

    > *'… the rules governing the use of Bulk Personal Datasets are not defined in legislation'* (§157).

    b) The ISC "*has a number of concerns*" about the lack of a proper legal regime for the collection and use of Bulk Personal Datasets. In particular:

[1] In fact, this was incorrect. The collection of BCD under section 94 TA was not avowed until November 2015.

i) Excessive and unjustified secrecy: "*…until publication of this Report, the capacity was not publicly acknowledged, and there had been no public or parliamentary consideration of the related privacy considerations and safeguards*".

ii) No legislative rules, restrictions or penalties for misuse: "*The legislation does not set out any restrictions on the acquisition, storage, retention, sharing and destruction of Bulk Personal Datasets, and no legal penalties exist for misuse of this information*."

iii) No system of warrants, or ministerial approval: "*Access to the datasets… is authorised internally within the Agencies without Ministerial approval*" and "*Ministers are not required to authorise the acquisition or use of Bulk Personal Datasets in any way…*" (§158, 159), although Ministers are "*often, but not always*" consulted before acquisition of a new dataset (but not the use of the dataset) (§159).

iv) No statutory oversight of the use of Bulk Personal Datasets (§160). That defect was only rectified on the day that the ISC Report was published (see below).

32. On the publication of the ISC Report, the Prime Minister signed the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015 [A1/16]. The Direction placed the review of Bulk Personal Datasets by the Intelligence Services Commissioner onto a statutory basis.

33. Bulk Personal Datasets were defined in the Direction as follows:

> '*5. For the purposes of this Direction, a bulk personal dataset means any collection of data which:*
>
> *a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;*
>
> *b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;*
>
> *c. Is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies.'*

34. BPD are shared with foreign security and intelligence services. It is assumed for the purposes of this hearing (the true position being neither confirmed nor denied) that they are also shared with other UK government agencies for non national-security purposes. As the ISC noted, once data has been shared, control over it is lost ("*… while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets*") (§163 [A4/79]).

D. Legal Framework

35. By section 6 of the Human Rights Act 1998 [A1/6], it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates the European Convention on Human Rights ("ECHR").

36. Article 8 ECHR provides:

> '1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*'

37. There are therefore four questions:

a) Is the relevant right engaged?

b) Does the interference comply with the requirement of legal certainty imposed by the relevant Article?

c) Is the interference in pursuit of a legitimate aim?

d) Is the interference proportionate to the goal (i.e. "*necessary in a democratic society…*")?

Engagement of rights

38. Article 8 of the ECHR is engaged. The acquisition, retention, use and sharing/dissemination of a large database of information or the use of a section 94 TA direction to accumulate personal data amounts to a serious interference with the Article 8 right of privacy. See the judgment of the Grand Chamber of the CJEU in Case C-293/12 *Digital Rights Ireland* [A3/62] at §§33-34 and the judgment of the Grand Chamber of the ECHR in *S & Marper v UK* (2008) [A3/54] at §§70-86. This Tribunal is bound so to conclude.

Legal certainty

39. Any interference with Article 8 must be "*in accordance with the law*" (see Article 8(2)). This requires more than merely that the interference be lawful as a matter of English law: it must also be "*compatible with the rule of law*": *Gillan v United Kingdom* (2010) 50 EHRR 45 [A3/58] at §76. There must be "*a measure of legal protection against arbitrary interferences by public authorities*", and public rules must indicate "*with sufficient clarity*" the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

40. Numerous cases have addressed this requirement in the context of secret surveillance and covert information gathering:

a) In *Malone v United Kingdom* (1985) 7 EHRR 14 [A3/46], the Court held that the legal regime governing interception of communications "*must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*" (at § 67). It must be clear "*what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive*" and the law must publicly indicate "*with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*" (at § 79).

b) In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007) [A3/52], the Court held at §75:

> '*In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated …*'.

c) These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the "*procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*" (*Liberty v UK* (2009) 48 EHRR 1 [A3/55] at §69).

d) In *Weber & Saravia v Germany* (2008) 46 EHRR SE5 [A3/53] the ECtHR held at §§93-94:

> '*The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures … Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.*'

e) In *Weber* the Court at §95 set out minimum safeguards (with numbers and spacing added for clarity):

> '*In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power:*
>
> > *[1] the nature of the offences which may give rise to an interception order;*
> >
> > *[2] a definition of the categories of people liable to have their telephones tapped;*
> >
> > *[3] a limit on the duration of telephone tapping;*

> *[4] the procedure to be followed for examining, using and storing the data obtained;*
>
> *[5] the precautions to be taken when communicating the data to other parties; and*
>
> *[6] the circumstances in which recordings may or must be erased or the tapes destroyed.'*

f) *Weber* was an interception case, but the principles in *Weber* have wider application to cases involving surveillance of all kinds. The touchstone is whether the degree of interference with privacy is comparable to that involved in interception of communication or communications data. (See *RE v UK* [A3/60] at §130: "*the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference*").

g) Further, in *Szabo & Vissy v Hungary* (Application 37128/14, 12 January 2016) [A3/61], the ECtHR indicated that "*[t]he guarantees required by the extant Convention case-law on interception need to be enhanced*" in view of the impact of "*cutting-edge technologies*" on the scale and effect of such interception. It is no longer adequate simply to apply *Weber*. The Tribunal should consider what additional safeguards are required to provide protection against arbitrary conduct in the context of new surveillance techniques.

41. The ultimate issue is whether the legal framework in fact contains adequate safeguards and is sufficiently foreseeable to the public. As David Anderson QC noted in *A Question of Trust* [A4/80], echoing the principles of the ECtHR case law:

> '*13.5 … in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency: not just fashionable buzz-words, but the necessary foundation for the trust between government and governed upon which the existence of coercive and intrusive powers depends in a modern democracy*'.

In consequence:

> '*13.18… if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed*'.

42. In *Watson & Others* [A3/63], Advocate General Saugmandsgaard Øe cited James Madison writing in 1788 to the same effect:

> *'1. If men were angels, no government would be necessary. If angels were to govern men, neither internal nor external controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.'*

43. Applying these principles, the ECtHR has repeatedly held that the intercept and surveillance practices of the UK did not include sufficient public and binding safeguards and did not comply with the "*in accordance with the law*" requirement. See,

for example, *Malone v UK* [A3/46], *Liberty v UK* [A3/55], *Khan v UK* [A3/51] and *RE v UK* [A3/60]. Similarly, in this Tribunal see *Liberty/Privacy No. 1* [A2/38] on the foreseeability of intelligence sharing and *Belhaj* [A3/42] in the IPT on legal professional privilege (by concession).

44. It is no answer to assert that individual decisions on retention or use made under the legal framework could be proportionate. See the judgment of Lord Reed in *R (T) v Chief Constable of Greater Manchester* [2014] UKSC 35, [2014] 3 WLR 96 [A2/39] at §114:

> '*Determination of whether the collection and use by the state of personal data was necessary in a particular case involves an assessment of the relevancy and sufficiency of the reasons given by the national authorities. In making that assessment, in a context where the aim pursued is likely to be the protection of national security or public safety, or the prevention of disorder or crime, the court allows a margin of appreciation to the national authorities, recognising that they are often in the best position to determine the necessity for the interference. As I have explained, the court's focus tends to be on whether there were adequate safeguards against abuse, since the existence of such safeguards should ensure that the national authorities have addressed the issue of the necessity for the interference in a manner which is capable of satisfying the requirements of the Convention. In other words, in order for the interference to be "in accordance with the law", there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. Whether the interference in a given case was in fact proportionate is a separate question.*'

45. If the Tribunal took a different approach in *Greennet* [A3/44], that approach is incorrect. Where powers are exercised in secret, the case law of the ECHR stresses the importance of ensuring that adequate safeguards are in place. It is not sufficient that a power is capable of being exercised proportionately in a particular case. What the national legislation must do is publicly ensure that there are sufficient binding rules as to prevent arbitrary use of the power, and that sufficient mandatory safeguards are in place to ensure that a power is exercised proportionately.

46. Lord Reed also emphasised at §115 in *R (T)* [A2/39] that whether a provision is "*in accordance with the law*" is not a matter on which a court should give deference to the decision maker (a matter in which his views were the majority: see [158]):

> '*Whether a system provides adequate safeguards against arbitrary treatment, and is therefore* "in accordance with the law" *within the meaning of the Convention, is not a question of proportionality, and is therefore not a matter in relation to which the court allows national authorities a margin of appreciation.*'

Domestic legal regime

47. The collection and onward disclosure of Bulk Personal Datasets may be carried out under section 19 of the Counter Terrorism Act 2008 [A1/9]. Section 19 provides (emphasis added):

> *'(1) A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions.*

(2) Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.

(3) Information obtained by the Security Service for the purposes of any of its functions may be disclosed by it –

(a) for the purpose of the proper discharge of its functions,

(b) for the purpose of the prevention or detection of serious crime, or

(c) for the purpose of any criminal proceedings.

(4) Information obtained by the Secret Intelligence Service for the purposes of any of its functions may be disclosed by it –

(a) for the purpose of the proper discharge of its functions,

(b) in the interests of national security,

(c) for the purpose of the prevention or detection of serious crime, or

(d) for the purpose of any criminal proceedings.

(5) Information obtained by GCHQ for the purposes of any of its functions may be disclosed by it –

(a) for the purpose of the proper discharge of its functions, or

(b) for the purpose of any criminal proceedings.

(6) A disclosure under this section does not breach –

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed).'

48. Receipt or disclosure of information pursuant to section 19 of the 2008 Act does not require any warrant or other external authorisation, regardless of the private or sensitive nature of the information.

49. Other powers may also be used to collect information for storage in a Bulk Personal Dataset, such as:

a) the warrant regime governing intercept and related communications data in Part I Chapter I of RIPA [A1/7];

b) sections 5 or 7 of the Intelligence Services Act 1994 [A1/4]; or

c) section 94(1) of the TA 1984 [A1/1].

50. In general terms, for all public and private bodies the retention and processing of personal data is regulated by the Data Protection Act 1998 ("the DPA") [A1/5]. However, the Agencies enjoy a wide exemption from the DPA where a national

security certificate has been made under section 28 of the DPA. For example, GCHQ's certificate [3/17-20] provides for the following exemption:

PART A			
Column 1		Column 2	
1.	Personal data processed in the performance of the functions described in section 3 of the Intelligence Services Act 1994 ("ISA") or personal data processed in accordance with section 4(2)(a) ISA.	i) ii) iii) iv) v)	Sections 7(1),10 and 12 of Part II; Sections 16(c), 16(e), 16(f),17,21,22 and 24 of Part III; Part V; the first data protection principle; the second data protection principle;
2.	Personal data relating to the vetting of candidates, staff, contractors, agents and other contacts of GCHQ in accordance with the Government's security and vetting guidelines and policy including but not limited to:	vi) vii)	the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and the eighth data protection principle.

51. The Data Protection Principles are as follows. The principles in bold type are abrogated by the Certificate:

> ***'1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—***
>
> ***(a) at least one of the conditions in Schedule 2 is met, and***
>
> ***(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.***
>
> ***2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.***
>
> *3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
>
> *4. Personal data shall be accurate and, where necessary, kept up to date.*
>
> *5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
>
> ***6. Personal data shall be processed in accordance with the rights of data subjects under this Act.***
>
> *7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
>
> ***8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'***

52. The statutory regime governing the obtaining of communications data is set out in Part I of RIPA [A1/7]. RIPA sets out two routes:

a) First, under Part I, Chapter I as "*related communications data*" obtained by or in connection with interception (sections 5(6)(b) and 20). Only a limited group of agencies can obtain an interception warrant (see section 6(2)). The grounds for obtaining such data are limited to national security, serious crime and the economic well-being of the UK.

b) Secondly, under Part I, Chapter II. A wider group of agencies can obtain communications data under Chapter II. The grounds on which communications data can be obtained are also wider (section 22(2)). The Chapter II scheme provides for two methods: the public authority may be authorised to obtain the data itself under section 22(3), or it may require a telecommunications operator to obtain and disclose the data under section 22(4). The Chapter II scheme contains some safeguards:

   i) The authorisation or notice must be granted by a designated person. Designated persons must be of prescribed rank (section 22).

   ii) An authorisation or notice must be granted in writing, or in some other form that produces a record (section 23).

   iii) The Secretary of State retains control over the use of Chapter II. She may by order impose restrictions on the circumstances and purposes for which authorisations may be granted or notices may be given (section 25(3)).

   iv) There is review of the exercise and use of the powers by the Interception of Communications Commissioner (section 57(2)(b)).

53. The Acquisition and Disclosure of Communications Data Code of Practice ("the Code") [A4/75] contains additional safeguards applying to Part I, Chapter II. The current (March 2015) Code contains the following requirements:

a) There must be a detailed (usually written) application by a party, the applicant, to the Designated Person (i.e. the decision-maker) explaining the necessity and proportionality of acquiring the requested communications data, considering collateral intrusion and possible unintended consequences (paragraph 3.5).

b) There must be training in human rights principles and the legislation for the Designated Person (paragraphs 3.8-9).

c) An expert officer (the "Single Point of Contact") gives the Designated Person advice (paragraph 3.11). The SPoC must provide "*objective judgement and advice to both the applicant and the designated person*" and form the function of a "*guardian and gatekeeper… ensuring that public authorities act in an informed and lawful manner*" (paragraph 3.22). The SPoC must review all applications and draft notices, assure Designated Persons that they are lawful and free from error, and give advice on necessity, proportionality, collateral intrusion and unintended consequences (paragraph 3.22).

   i) The SPoC and the Designated Persons must usually be different people (paragraph 3.27). The applicant and the Designated Person "*must never*" be the same individual (paragraph 3.28).

ii) Except in certain urgent cases, the Designated Person must be independent from the relevant operation and investigation (paragraphs 3.12-3.15).

iii) The result is that three separate individuals will usually review any application: the applicant, the SPoC and the Designated Person.

d) An authorisation or notice is valid for a maximum of 1 month (paragraph 3.51). It may be renewed for a further month by the giving of a further authorisation or notice (paragraph 3.55). Notices or authorisations must be cancelled, in writing, once no longer necessary (paragraphs 3.58-60).

e) Where communications data is sought to determine a journalist's source, all law enforcement agencies must use PACE 1984 to obtain a production order from a judge, not RIPA (paragraph 3.78). This provision does not apply to the Agencies or in cases involving a risk of immediate threat to human life (paragraph 3.83). The Agencies approve access to journalistic source material (and legally privileged material) internally.

f) Local authorities must obtain prior judicial approval from a magistrate (paragraph 3.85 and following), pursuant to sections 23A-B of RIPA [A1/7], as inserted by the Protection of Freedoms Act 2012.

g) There is a duty to keep detailed records, including statistical information (paragraph 6.5-6).

h) Errors must be reported to the Commissioner (paragraph 6.15).

i) The Commissioner may inform the affected individual in limited circumstances, to enable a complaint to the IPT (paragraphs 6.22 and 8.3).

E. Submissions

Issue 1: Section 94 under domestic law

54. On a proper construction of section 94 [A1/1], it cannot lawfully be used to obtain BCD. Reading section 94 alongside Part I of RIPA [A1/7], BCD should have been obtained (if at all) by an authorisation or warrant under RIPA. The general words in section 94 do not permit activity for which authorisation should have been sought under specific provisions designed by Parliament to govern that conduct.

55. The Respondents accept that they could not lawfully use section 94 to:

a) intercept content (under Part I, Chapter I of RIPA); or

b) carry out property interference (under the Intelligence Services Act 1994 or the Police Act 1997) (Amended Open Response, §198 [CORE/A2/45]).

The concession is rightly made. An attempt to use section 94 to intercept or carry out property interference in circumstances where Parliament provided an alternative specialist statutory scheme would be unlawful - it would subvert the dedicated statutory procedure. But the Respondents do not accept where their concession logically leads. Having accepted that section 94 cannot be used where there is a later specialist scheme in place, the Respondents still seek to contend that section 94 TA can be used to obtain communications data, in bulk.

56. The Secretary of State could not authorise interception of communications under TA once Parliament had provided a detailed regime accompanied by safeguards in RIPA. Even if the general power could have been used prior to specific legislation being passed, it cannot continue to be used that way after the passing of RIPA in 2000. The specialist scheme is the only lawful means to collect communications data.

57. It is also most unlikely that after RIPA, Parliament could have contemplated or intended section 94 to extend to collecting BCD. Section 94 applies only to public electronic communications networks. So it does not apply to providers of internet services such as Skype, Gmail, WhatsApp or other similar services. One of the purposes of RIPA was to provide a scheme that would cover internet services, whilst also offering additional safeguards. The partial nature of the coverage of section 94 makes it yet more implausible that Parliament intended this provision to be a work around to RIPA.

58. Indeed, if interception or the collection of communications data could lawfully be carried out under TA, the basis on which the UK defended cases such as *Kennedy v UK* [A3/50] in respect of individual surveillance and *Liberty v UK* [A3/55] – namely that RIPA provided a complete and comprehensive code of the relevant interception powers, together with the safeguards thought appropriate by Parliament - would be falsified.

59. The effect of using s. 94 TA to obtain communications data or content is to circumvent the specific safeguards provided for by the legislation, in particular in RIPA Part I and the relevant statutory Codes of Practice approved by Parliament [A4/64-77].

60. For example, under s. 94 TA:

a) There is no Single Point of Contact, or requirement for approval by a Designated Person. The approval granted by the Secretary of State is generic, not operational.

b) There is no requirement for monthly re-authorisation.

c) There is no statutory oversight by a Commissioner.

61. The legal analysis is straightforward:

a) Where specific powers with relevant safeguards exist, it would absent a good reason be a misuse of power to use a general power without such safeguards. Where Parliament has provided a *lex specialis*, it frustrates Parliament's scheme to use a general power. That is particularly the case where the general power is being exercised entirely in secret, not disclosed to Parliament.

b) The principle is an old one, and was set out by Romilly MR in *Pretty v Solly* (1859) 26 Beav 606 [A1/18] in these terms (at 610):

> *"The general rules which are applicable to particular and general enactments in statutes are very clear, the only difficulty is in their application. The rule is, that wherever there is a particular enactment and a general enactment in the same statute, and the latter, taken in its most comprehensive sense, would overrule the former, the particular enactment must be operative, and the general enactment must be taken to affect only the other parts of the statute to which it may properly apply."*

c) Precisely the same analysis applies where the specific statute follows an earlier more general statute. For example, in *R v Director of the Serious Fraud Office ex p Smith* [1993] AC 1 (HL) [A1/22], the House of Lords held that the general principle regarding the accused's right to silence (as protected in the PACE Code) had been abrogated by the subsequent, more specific provisions in the Criminal Justice Act 1987. Lord Mustill held (at pp.43-44):

> *'For these reasons I conclude that as a matter of interpretation the powers of the Director do not cease, as regards the questioning of the person under investigation, when he is charged; that the principle of common sense, expressed in the maxim* generalia specialibus non derogant*, entails that the general provisions of the Code yield to the particular provisions of the Act of 1987 in cases to which that Act applies; and that neither history nor logic demands that any qualification of what Parliament has so clearly enacted ought to be implied.'*

d) Similarly, in *R v Liverpool City Council, ex p Baby Products Association* [2000] BLGR 171 (QB) [A1/24], Lord Bingham CJ held at 178E-F:

> *'A power conferred in very general terms plainly cannot be relied on to defeat the intention of clear and particular statutory provisions.'*

In that case, a detailed statutory code, containing various procedural safeguards, governing the enforcement of consumer protection legislation, would have been undermined by the use of a local authority's general powers to publish information under the Local Government Act 1972. The

local authority was therefore held to have acted unlawfully in using the more general powers and avoiding the various procedural safeguards. The principle has also recently been applied in the context of information gathering powers in *R (W) v SS for Health* [2015] EWCA Civ 1034 [A3/43], at [57]-[62] per Lord Dyson MR (the debate being which of the two powers were more specific so as to oust the other).

e) In *Re McE* [2009] 1 AC 908 [A2/34], the House of Lords held that RIPA permitted covert surveillance of communications between persons in custody and their legal advisers, despite earlier general legislative provisions protecting privilege by referring to '*private*' consultation. Lord Carswell at [98]-[105] considered the application of the principle of implied repeal; his lordship noted (at [98]) that the question is one of '*legislative intention, which the courts endeavour to extract from all available indications*'. It was clear that Parliament had intended such consultations to fall within the RIPA regime, which was designed to be comprehensive (accepting a submission to this effect of the Secretary of State: see [70]). It is notable that RIPA came into force on the same day as the HRA 1998 [A1/6] and was intended to provide a Convention compliant scheme, unlike TA 1984 (see [62]).

f) The issue can also be analysed by reference to the principle of legality. The principle seeks to ensure that important rights are not abrogated by a statute whose "*full implications […] may have passed unnoticed in the democratic process*" (per Lord Hoffmann in *Simms* [A1/25]).

g) The principle of legality continues to apply in national security cases. In *Ahmed v HM Treasury* [2010] 2 AC 534 [A2/36], a case concerning the freezing of assets belonging to individuals reasonably suspected of involvement in terrorism, the principle was applied with full force:

i) In the Court of Appeal, the Treasury made submissions concerning the effect of general or ambiguous words in the United Nations Act 1946, and stressed "*the preventative nature of the regime introduced by the Security Council and the importance of avoiding terrorism*"; Sir Anthony Clarke MR held at [48]: "*For my part, I would not accept those submissions. I can see that the widest possible power might be desirable from the Government's point of view. I can also see that the public might take the same view. However, the principles which I have just stated are of fundamental importance.*"

ii) The Supreme Court agreed. For example, Lord Hope expressly held at [75] that any interference with property required clear legislative words, citing the general warrant cases: "*the right to peaceful enjoyment of his property, which could only be interfered with by clear legislative words*: Entick v Carrington (1765) 19 State Tr 1029 , 1066, *per Lord Camden CJ… these rights are embraced by the principle of legality, which lies at the heart of the relationship between Parliament and the citizen. Fundamental rights may not be overridden by general words. This can only be done by express language or by necessary implication*". Arguments that national security cases should be treated differently were firmly rejected [79-80], noting the "*dangers that lie in the uncontrolled power of the executive*". Such reasoning makes the principle implying exclusive recourse to the dedicated, specific regime for cases whose facts fall within it all the

stronger in a case substantially affecting fundamental rights, even where the context is national security.

h) Parliament cannot be taken to have abrogated the right to privacy in TA 1984 by the use of general words.

62. Following the passing of the Data Retention and Investigatory Powers Act 2014 ("DRIPA") [A1/11], the position is *a fortiori*. Section 1(6) of DRIPA provides:

> *'A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except –*
>
> *(a) in accordance with –*
>
> *(i) Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 (acquisition and disclosure of communications data), or*
>
> *(ii) a court order or other judicial authorisation or warrant, or*
>
> *(b) as provided by regulations under subsection (3).'*

63. The purpose of DRIPA was to ensure that communications operators retained limited categories of information (set out in the Data Retention Regulations 2014) to be able to respond to lawful requests. Parliament's scheme was that data would be retained securely by telecommunications operators and only disclosed in response to a RIPA authorisation, or judicial authority. These arrangements are supported by a statutory code of practice (made under section 2(4)(c) of DRIPA), and would be frustrated if the same result could be achieved by another means. Even the limited and inadequate safeguards in DRIPA and RIPA would be avoided if section 94 could be used to achieve the same result (e.g. time limits in section 1(5) and disclosure in section 1(6)).

64. The assumed facts also demonstrate the potential for circumvention of RIPA. GCHQ collect BCD under section 94 for national security purposes. GCHQ could not obtain a section 94 authorisation for other purposes. Despite that, GCHQ is assumed to share section 94 BCD with HMRC and the NCA to assist in criminal investigations. But the data could not lawfully have been authorised for collection under section 94 for this purpose, and HMRC and the NCA could have requested and obtained communications data themselves under RIPA. The effect is to circumvent the protection of the Designated Person, the SPoC, the Commissioner and the other safeguards in the Code.

65. Nothing in the above submissions deprives section 94 of practical utility. There are a number of such lawful uses of section 94 identified in the Burnton report [A4/82] ("*A notice might typically require… services to support secure communications by the security and intelligence agencies… the confidential provision of services… maintaining a pool of trusted staff* [or] *provision in emergencies for civil contingency purposes*" §9.3-9.5). Indeed, the Investigatory Powers Bill [A1/17] proposes repealing section 94 TA and replacing it with a narrowed power to give a (judicially approved) national security notice which does not give access to content or communications data (clause 225).

66. The Respondents' Amended Open Response asserts that the use of s. 94 to require the production of BCD '*was plainly within the contemplation of Parliament*' (§200 [CORE/A2/45-46]). This is incorrect: this novel and aggressive purported use of

section 94 was not implemented for almost 15 years after the passage of the legislation. In 1984 there were only a small number of mobile telephones, no internet in the modern sense and few networked computers. There is no clue in the wording of section 94 or public statements by HM Government that such use might be made of section 94.

67. The proper construction is that the *lex specialis* of RIPA ousts the *lex generalis* in section 94 of the TA. This domestic analysis is supported by both the interpretive obligation in section 3 HRA and EU law. The section 94 TA regime as applied to BCD breaches Article 8 rights and is contrary to the Charter and the e-Privacy Directive. Both section 3 HRA and the *Marleasing* principle of interpretation require the Tribunal to construe section 94 narrowly so as to be compatible with fundamental rights.

Issue 2: Is the section 94 Regime in accordance with the law?

Prior to avowal

68. Prior to the avowal of the use of section 94 TA [A1/1] to collect bulk communications data (on 4 November 2015), the scheme was not in accordance with the law, applying the case law and principles set out above:

a) The regime was entirely secret and therefore insufficiently foreseeable. No information at all was in the public domain beyond the existence of a generally worded power in section 94. The power gives no indication that collecting everyone's communications data in bulk might be permitted. Such general powers accompanied by aggressive and expansive interpretations of the law in secret (and thus away from debate or scrutiny) were strongly criticised by David Anderson QC [A4/80].

b) There was no public information about the use of section 94 from which it could be deduced that it was being used to collect the communications data of everyone in the UK. Most people reading the statutory scheme and the Codes of Practice [A3/64-A4/77] would:

i) think that the scheme for obtaining communications data operated under RIPA [A1/7] not TA 1984; and

ii) not expect the RIPA scheme to be circumvented by an obscure and general power.

The availability of a bare statutory power to issue a direction that cancels any unlawfulness is self-evidently not an adequate safeguard against arbitrary conduct (in correspondence with Sir Swinton Thomas on 18 October 2004 [3/430-433] GCHQ accepted that "*it is* arguable *that s. 94 is insufficiently precise so as to make the access of any data obtained pursuant to any directions issued under that section not in accordance with the law…*" but did not analyse the authorities or principles any further).

c) There was no statutory oversight of section 94 directions.

d) No central or accessible record has been maintained of the section 94 directions made by the various Secretaries of State. Sir Stanley Burnton was very critical (§5.10, Burnton Report [A4/82]). It was not until November 2015 that IOCCO had managed to compile a list of the full set of section 94 directions (Response to RFI, §29 [CORE/A4/9-10]).

e) Section 94 directions do not expire, can be given orally, and are not limited in time. In contrast, a warrant must be in writing and it only has a limited period of validity, as required by *Weber* [A3/53]. There is no statutory provision for the review of directions.

f) There was no Code of Practice or other public set of rules or policies governing the acquisition, use, retention, disclosure, storage and deletion of personal data under section 94. The *Weber* criteria are not met. Nor was there even power to issue a Code of Practice. The absence of a Code was criticised at §4.14 of the Burnton Report [A4/82], where Sir Stanley explained the real

safeguards that a Code would offer and the significant omissions in the existing scheme (at §4.15).

g) There were no procedures in place to protect legally privileged material, or to prevent the use of section 94 data from being used to uncover a journalistic source. It appears likely that (as in other cases) the Agencies operated under the misapprehension that communications data could not be legally privileged. The absence of safeguards to protect such material is particularly serious, and contrary to well-established Convention case law. See the Advocate General's summary in *Watson & Others* [A3/63] at §235.

h) Until recently, the oversight provided by the Commissioners (and the information provided by the Agencies to the Commissioners) was inadequate. Sir Stanley Burnton's report on section 94 fairly sets out the limits of past oversight [A4/82]. In particular:

i) "*… from 2004 to 2015, the Commissioner's oversight was not provided on express, agreed, terms*" (Response to Supplemental RFI, §79 [CORE/A9/21-22]).

ii) Past oversight was "*on a limited basis*" because "*it was only concerned with the authorisations to access the communications data… not… the giving of the section 94 directions… or the arrangements for the retention, storage and destruction of the data*" (Burnton Report, §2.5 [A4/82]).

iii) Sir Swinton Thomas made significant legal errors in his analysis of the legal regime, and thus was unable to make a proper assessment of the propriety of the use of section 94 TA (see Sir Stanley Burnton's criticisms at paragraph 21 above):

a) He (as the Respondents' now accept) wrongly concluded that a database that is initially anonymous, but which can be deanonymised raises no Article 8 issue (Supplemental RFI, Responses 1-5 [CORE/A9/2], letter of 8 June 2004 [3/424]).

b) Sir Swinton Thomas' analysis of the domestic *vires* issue is very brief and inadequate, and was limited to adopting arguments about the practical benefits of avoiding monthly authorisation and discouraging law enforcement agencies from creating their own BCD databases (letters of 22 June and 6 July 2004 [3/426-428]). None of the pertinent domestic principles of construction, set out above, was even considered.

c) Sir Swinton failed to consider any of the Strasbourg case law on Article 8 or the applicable EU law provisions in the e-Privacy Directive.[2]

iv) Sir Mark Waller was informed by GCHQ that section 94 was used to enable "*data… which CSPs are willing to provide, but there is no other*

[2] The final transposition date for the e-Privacy Directive was 31 October 2003, prior to Sir Swinton Thomas' advice.

mechanism by which we can support that provision with a form of legal authorisation" (29 March 2011, §10 [3/527]). In fact, GCHQ's (and Sir Swinton Thomas') view was that RIPA was a lawful alternative route to obtain BCD. Sir Mark Waller does not appear to have challenged GCHQ's analysis.

v) No audit was carried out of the use of section 94 data ("*Sir Mark Waller… looked at the overall use and purpose of the data rather than the specific requests made of the data*": Response to Supplemental RFI, §84 [CORE/A9/23-24]). Sir Paul Kennedy took the same limited approach (Response to Supplemental RFI, §88 [CORE/A9/24-25]). This was not remedied until December 2015, when IOCCO were provided with access to the relevant electronic systems and they carried out sampling and query-based analysis (Response to Supplemental RFI, §88 [CORE/A9/24-26]).

vi) It was not until February 2015 that "*oversight was extended to cover the necessity and proportionality of section 94 directions made by the Secretary of State and the retention, storage and destruction arrangements for the BCD*" (Response to RFI, §29 [CORE/A4/9-10]). Even then, oversight could not begin because the Commissioner explained that he would "*require extra staff (and possibly technical facilities) to be able to carry out this oversight properly*" (Response to RFI, §29 [CORE/A4/9-10]).

vii) In consequence, significant errors in procedure, such as failures to comply with the Code of Practice by 63 analysts and 25 Designated Persons, were not identified by the Commissioners (Response to Supplemental RFI, §91 [CORE/A9/26] and Amended Security Service Witness Statement, §148[3] [CORE/B2]).

i) There is no requirement for judicial or independent authorisation. In *Szabo & Vissy v Hungary* (Application 37128/14, 12 January 2016) [A3/61] the ECtHR held at [77] that "*supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees*". It noted at [69] that the earlier case of *Kennedy v United Kingdom* (2011) 52 EHRR 4 [A3/59], in which the ECtHR had held that a regime in which interception warrants were issued by the Secretary of State was compatible with Article 8, had concerned a tightly circumscribed power – noted by the ECtHR in *Kennedy* at [160] as requiring the identification of one specific person or set of premises as the subject of the warrant – and was therefore not applicable where the power could potentially "*be taken to enable so-called strategic, large-scale interception*". The Advocate General in *Watson & Others* [A3/63] reached the same conclusion: "*the intervention of an independent body prior to the consultation of retained data, with a view to protecting persons whose data are retained from abusive access by the competent authorities, is to my mind imperative*" (§236).

j) There is no procedure to notify victims of any use (still less misuse) of BCD, so that they can seek an appropriate remedy before the Tribunal. See the

[3] The promised supplemental witness statement giving further information about the errors at the Security Service has not yet been produced (Amended Security Service Witness Statement, §151).

Opinion in *Watson & Others* [A3/63] at §49 and §236. Without such a mechanism, and in the absence of independent or judicial authorisation, a victim of an abuse of rights has no prospect of ever securing a remedy. The Advocate General's analysis in *Watson & Others* is correct (at § 236):

> *'… from a practical point of view, none of the three parties concerned by a request for access is in a position to carry out an effective review in connection with access to the retained data. Competent law enforcement authorities have every interest in requesting the broadest possible access. Service providers, who will be ignorant of the content of any investigation file, are incapable of checking that requests for access are limited to what is strictly necessary and persons whose data are consulted have no way of knowing that they are under investigation, even if their data is used abusively or unlawfully…'.*

69. The position is therefore *a fortiori* to the facts of *Liberty & Privacy International No 2* [A3/41] at [20] where no procedures were in the public domain about information sharing, but the fact of the existence of arrangements was known. Here, it was not known if there were proper arrangements governing section 94, and the contents of any arrangements were entirely secret (cf. sections 15-16 RIPA).

70. The position is also worse than the pre-IOCA 1985 days of intercept considered by the ECtHR in *Malone* [A3/46]. See *Liberty v UK* [A3/55] where there was no Code of Practice under IOCA 1985, nor any public safeguards or limits on a strategic anti-terrorism intercept power. The subsequent introduction of the RIPA Interception Code of Practice demonstrated the inadequacy of what went before. The ECtHR found a breach of Article 8 ECHR.

After avowal and publication of the section 94 handling arrangements on 4 November 2015

71. On 4 November 2015, the use of section 94 to collect BCD was avowed. Handling Arrangements [3/130-137 and 3/314-327] were published on the same day.

72. The Arrangements were materially misleading:

a) They do not disclose that the Security Service operates an entirely different procedure to GCHQ when accessing BCD.

b) They fail to disclose that GCHQ was collecting Subscriber Information until shortly before the publication of the Arrangements (paragraph 2.2 [3/130]).

c) They claim that the data collected does not include 'Internet Connection Records'. However internet companies have been required to produce internet data and that information has now been re-used for non-national security purposes (see paragraph 20.f) above).

73. Further, in addition to the points made above, the Arrangements are and remain inadequate:

a) The extensive recommendations made by Sir Stanley Burnton have not been implemented and the concerns he raised remain (Burnton Report, §11-12 [A4/82]).

b) GCHQ do not operate any of the safeguards of a RIPA Part I Chapter II process [A1/7]. There is no SPoC or Designated Person. Officers are able to have direct access to data without approval from a senior officer. Sir Mark Waller expressed concern during a meeting on 12 November 2014 ("*Sir Mark was concerned that he had said in his annual report that staff cannot act independently, but the… case demonstrated that this was not true*") [3/523].

c) The Security Service adopt a process under Part I Chapter II for access to data. If the Security Service can adopt such a procedure, there is no good reason why it cannot also be adopted by GCHQ.

d) Further, the Security Service do not properly comply with the Communications Data Code of Practice:

i) As the Commissioner explained, "*there is no evidence of DPs complying with para. 3.11 of the CoP* [necessity] *(indeed as mentioned in a preceding baseline many are not recording considerations at all when approving applications*" (December 2014 Inspection Report [3/444]).

ii) The provisions requiring that the Designated Person be independent of the relevant investigation have not been implemented or followed, despite both the Interception of Communications Commissioner and the Secretary of State requesting compliance with the Code. The Commissioner's December 2015 inspection report states at p. 19 [3/446]:

> *'All other applications (i.e. the majority) are forwarded to the applicant's line manager for appeal. The line managers are not independent from the operations or investigations for which they are granting authorisations or giving notices.'*

iii) The Commissioner rejected the suggestion that this was not possible due to urgency or reasons of security (p. 19 [3/446]):

> *'One of the exceptions for independence… refers to ongoing operations or investigations immediately impacting on national security issues where the public authority is not able to call upon a DP who is independent. We do not consider that this exception applies to the routine applications submitted by the Security Service as in these cases there is no immediacy and the public authority has enough DPs of the prescribed ranks to be able to call upon DPs who are independent.'* (emphasis in original)

iv) The Commissioner then rejected various points relied on by the Security Service in correspondence with the Home Secretary.[4] The

[4] The correspondence with the Home Secretary does not show the Security Service in a good light. Andrew Parker's letter of 19 March 2015 concludes "*there does not appear to be a pressing litigation or reputational requirement to commit to make these changes now and we can therefore see no obvious gain in doing so*" [3/455]. As in other cases before the Tribunal, the Agencies have only begun to make necessary changes to their procedures when there is a "*pressing litigation or reputational requirement*". It is unfortunate that the pressure of continued litigation or adverse publicity, rather than a culture

Commissioner concluded that the non-compliance was now "*even more critical*" and directed that the Service "*must*" comply with the Code of Practice [3/447]. To date, this has not yet happened. Indeed, the Director's letter of 18 December 2015 makes clear that the agency has no intention of complying with the requirements of the Code [3/460-462].

v) The fact of non-compliance with the Code was kept secret until recently. Further, the Security Service falsely stated that it had received an exemption from the Code by authority of the Home Secretary and the Interception of Communication Commissioner (neither of whom have such authority – only Parliament may authorise an amendment to the Code). GLD's letter of 11 April 2016 [3/417-418] states:

> *'… paragraph 2 of the Security Service's warrantry briefing note of 27 October 2015 contains a factual inaccuracy which the Security Service thought it important to correct. That paragraph states:*
>
> > *"Whilst the Code also states that *all* CD requests should be authorised by DPs who are independent of the investigation, MI5 uniquely and temporarily has an exemption granted by the Home Secretary from this requirement. This exemption is based on the National Security exemption provided for in the Code. This approach has also been agreed with the relevant oversight body, IOCCO, and the Interception of Communications Commissioner."*
>
> *… it was not correct to say that the Home Secretary had granted an exemption or that the Commissioner or IOCCO had approved it.'*

The reason for the error has not been explained.

vi) Designated Persons do not have to give any reasons for their decisions (RFI 24), although it is recommended they "*consider adding brief comments*" when rejecting an application, approving a large application, or when there is unusual interference with privacy or collateral intrusion [3/279-80]. The absence of reasons makes auditing very difficult.

vii) That procedure was changed in January 2015 requiring ("*you must*") the use of a specified form of words where the request would obtain data about persons in sensitive professions (RFI 25) [3/286].[5] The

---

expecting action within the law, is what is required to secure compliance with the published Code of Practice.

[5] The definition of 'sensitive profession' is also inadequate. Lawyers are defined as "*barristers and solicitors only*" thus excluding (a) Fellows of the Institute of Legal Executives; (b) a Scottish advocate; (c) a clerk or paralegal who may have a privileged conversation with a client or witness. Medical doctors are defined as excluding "*dentists… nurses or mental health professionals*". A dentist is a medical professional subject to the same obligations of confidentiality as a doctor, and similarly

recitation of a formulaic set of words is not a good recipe for good decision-making.

e) Again, Sir Stanley Burnton was very critical in his Report [A4/82]:

> '*The designated persons undertaking this function are generally not independent from the investigations to which the requests they are authorising relate and they generally do not record any written considerations when approving such requests. Anyone familiar with* [the Code] *would recognise these two features as requirements when communications data is acquired using RIPA from communications service providers'* (§8.67).

f) Entire databases of BCD can be shared with foreign partners and GCHQ disclose entire databases of "*raw sigint data*" to "*industry partners*" who have been "*contracted to develop new systems and capabilities for GCHQ*" [3/476]. When this occurs, the usual safeguards are abrogated. For example, there is no requirement for each search to be explained and justified in writing. It is clear that at last one communications service provider has been sufficiently concerned to demand that foreign sharing of its customer data did not occur:

> '*In one case a PECN had asked the agency to ensure that that* [sharing with other jurisdictions] *did not happen and we were able to confirm that their data had not been shared with another jurisdiction. In other cases PECNs stated they would be very concerned if their data was shared with other jurisdictions without their knowledge'* (Burnton Report, §6.7 [A4/82])

g) Data obtained for one purpose (national security) is re-used for another. For example, an "*internet communications dataset*" has been obtained for "*UK cyber defence*" purposes, but has now been re-used for other purposes (see paragraph 20.f) above [CORE/A9/21]). Similarly, (on the assumed facts) data only obtained for national security reasons is repurposed to give access to HMRC and the NCA for criminal investigative purposes, thus circumventing the RIPA procedure and the Code.

---

lengthy training. The same applies to mental health professionals such as a chartered clinical psychologist.

Issue 3: Is the BPD regime in accordance with the law?

Prior to avowal

74. As with BCD obtained under section 94 TA [A1/1], prior to avowal the regime was not sufficiently foreseeable. The collection and holding of BPD was secret. There was nothing in the public domain to explain that the agencies used such highly invasive techniques or how bulk data was managed.

75. Nor were there adequate safeguards against arbitrary conduct. The Agencies were well aware of the problems. Robert Hannigan's 2010 review [3/563-573] sets out the difficulties candidly:

a) The Agencies' former Staff Counsellor (John Warne CB) queried the "*public defensibility (in case the need arises) of existing and planned holdings*" of BPDs. There had been "*concerns*" amongst staff "*regarding the unavowed nature of these holdings and a perceived absence of checks on their* use" (§1 [3/563]).

b) Mr Hannigan suggested that it was "*difficult to assess the extent to which the public is aware of agencies' holding and exploiting in-house bulk personal datasets, including data on individuals of no intelligence interest*" [3/564]. In fact, as at 2010, the only information about the Agencies' policies on data collection was set out in *Hewitt and Harman v UK* [A3/48]. That judgment suggested that the Security Service only kept individual files on people of legitimate interest. As Mr Hannigan accepted "*the extent to which this sharing takes places may not be evident to the public*" and the public would take a "*negative view*" if it were to be disclosed (§36 [3/571]).

c) Mr Hannigan noted that collecting BPD was "*less publicly defensible than traditional activity against identified intelligence targets…*" (§6 [3/564])

d) There was no oversight by the Information Commissioner (§30 [3/570]) (emphasis added):

> '*The Commissioners have no remit to scrutinise the acquisition, use and retention of most bulk personal data provided to the agencies voluntarily or acquired overtly from publicly or commercially available sources; or bulk communications metadata provided by CSPs.*'

e) Mr Hannigan recommended that "*an element of independent oversight of agency bulk-data holdings should be introduced*":

> '*37. Exploitation of bulk personal data by the agencies is arguably more difficult to defend publicly than other agency activities because a significant number of these bulk personal datasets are not subject to scrutiny by any of the Independent Commissioners… there is no statutory mechanism for independent oversight.*' [3/572]

Even though the recommendation for statutory oversight was agreed by the Agencies, the defect was only remedied in March 2015, 5 years later.

f) The Commissioners had been "*informally briefed*" on some bulk data holdings "*but not specifically on other holdings of bulk personal data*" (§30 [3/570]).

g) Mr Hannigan said that the Security Service "*has also briefed… the Investigatory Powers Tribunal… on bulk data techniques*" [3/570]. This briefing has not been disclosed. The briefing should be disclosed, along with any related correspondence.

h) The Home Secretary had requested further steps be taken: "*The Security Service has been tasked by the Home Secretary to work up a proposal to put oversight of its bulk data analysis techniques on a firmer footing…*" (§31 [3/570]).

i) Auditing was patchy: "*SyS and GCHQ carry out some auditing but do not systematically audit access to all non-targeted personal datasets*" (§33 [3/571]).

76. The October 2010 Security Service policy [3/154-165] is to similar effect, recognising the lack of foreseeability of the Agencies' BPD practices:

> '*… the fact that the Service holds bulk financial, albeit anonymised, data is assessed to be a HIGH corporate risk since there is no public expectation that the Service will hold or have access to this data in bulk*' (RFI, § 13 [3/162]).

77. As at May 2014, GCHQ had not commenced auditing its main corporate BPD tool (May 2014 ISC Inspection Report, p. 6 [3/546]). In May 2015, following the discovery by the Chief Inspector of IOCCO of a "*less than impressive paper trail*" and an "*issue of ownership*" of "*financial datasets*", GCHQ "*suspend*[ed] *acquisition of financial datasets until this is fully resolved and GCHQ's longer-term strategy for the acquisition and use of financial data has been agreed*" (Notes of 13 May 2015 [3/555-557] and email of 14 April 2015 [3/558]). The current position is unclear.

78. The internal procedures in each of the Agencies prior to avowal were inadequate:

a) At GCHQ (and possibly the other Agencies), unless the database contained "*real names*" (defined as "*at least the actual names of individuals*"), the dataset would not be treated as a BPD or be subject to review and approval procedures (RFI 7, p. 1 and 5 of 8 [3/90-97]). Accordingly, a database of financial transactions containing bank account numbers and sort codes, or a database of internet usage information by reference to home address or telephone number would be excluded from any review or oversight, even if the missing biographical information could easily be added.

b) At the Security Service, all commercially available datasets were excluded from the policy until "*late 2012*" (Amended Security Service Witness Statement, §70 [CORE/B2]). However, the use of such data (ordinarily subject to the DPA) may itself be intrusive, especially when combined with other data (see §71 [CORE/B2]). Nevertheless, there was no authorisation procedure or oversight.

c) At the Security Service, any BPD obtained under RIPA or ISA was excluded from the policy until "*Autumn 2013*" (Amended Security Service Witness Statement, §77 [CORE/B2]). Such material is likely to be highly intrusive with respect to persons of no intelligence interest.

d) At the Security Service, officials were instructed that "*the level of intrusion arising from the holding of data is generally assessed to be very limited*" (RFI 15 – March to November 2015 guidance [3/178]). This guidance cannot be

reconciled with the 2014 judgment of the CJEU in *Digital Rights Ireland* [A3/62], nor *MK v France* [A3/56] or *S v Marper* [A3/54], which all make clear that the retention of a database, even if not searched, is a serious interference with privacy calling for weighty justification. In *Watson & Others* [A3/63], the Advocate General noted "*General data retention obligations are in fact a serious interference with the right to privacy…*" (§128).

e) At SIS "*there is no requirement to enter the reason for a search before accessing the database*" (Hannigan Report, §18 [3/567] and Supplemental RFI Response, 41(d) [CORE/A9/12-13]). In contrast, GCHQ always required a brief three-part "*HRA justification*" specifying purpose, Joint Intelligence Committee requirement and a free-text explanation (Hannigan Report, §27 [3/569]).

f) There was significant abuse, including searches of high profile individuals "*that were not operationally justifiable*" (Supplemental RFI, Response 41(c) [CORE/A9/12]). At SIS, one individual "*was discovered to have searched bulk personal data in relation to a colleague on a number of occasions…*" (Amended SIS Witness Statement, §62 [CORE/B2]). Other staff carried out searches on themselves or their family to obtain biographical or travel detail (RFI 44 [3/395]).

79. Prior to 2010, there was no oversight of BPDs. The Security Service accepted internally that this was a problem ("*This* [non-statutory Commissioner] *oversight was put in place to cover a gap in oversight as well as to provide some assistance in addressing* [REDACTION] *Article 8 foreseeability* [REDACTION] *in relation to bulk personal datasets'* [3/214]).

80. Informal oversight by the Commissioners began at the end of 2010 and was inadequate. Initially it consisted only of limited and brief scrutiny of the authorisation forms:

a) In December 2011, Sir Paul Kennedy examined the authorisation forms for a single dataset. He did not examine the usage of any BPD, or audit any specific requests made (Response to Supplemental RFI §57 [CORE/A9/16]).

b) Sir Mark Waller's approach has been to:

> '*check… that the documentation (BPDAR) is in order, gives a good case for acquisition and retention of the dataset including necessity, proportionality and risk of collateral intrusion… He also discusses the operational use of those BPDs he has selected, with those who own the dataset… Thus, he looks at the overall use and purpose of the data rather than specific requests made of the data.*
>
> *Sir Mark has not been given samples of the queries run against any BPD*.' (Response to Supplemental RFI, §56 [CORE/A9/16]) (emphasis added).

c) Sir Mark Waller has not audited the use of any BPD, nor considered the increase in privacy interference when multiple datasets are used to create profiles. This is a significant omission, for the reasons given by the Respondents in the Closed Response ("*interaction between multiple datasets* [has the consequence] *that intrusion into privacy can increase*") (§4 [CORE/A6/2]).

d) None of the Commissioners appears to have questioned the exclusion of any dataset that omitted "*real names*" from the approvals process.

e) The Intelligence and Security Committee has not provided any oversight of BPDs save for its avowal of the capability in its report. It was only formally notified of BPDs in March 2014 (Response to RFI, §38 [CORE/A4/12]).

From avowal to the publication of the Arrangements

81. The BPD Direction [A1/16] placed oversight onto a statutory footing on 12 March 2015. However, until their disclosure in this case, no arrangements for such oversight were public. The scheme was not sufficiently foreseeable. The defects set out above (save for statutory oversight) remain.

From publication of the Arrangements to present

82. The current regime governing the acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct:

a) No warrant (whether judicial or otherwise) is required to obtain or interrogate a Bulk Personal Dataset, regardless of the sensitivity of the data obtained, or the size and scale of the dataset. For example:

i) If a BPD was obtained by intercept or property interference, a warrant would be required under RIPA [A1/7] or ISA [A1/4], involving the personal approval of the Secretary of State.

ii) But if a staff member of the data owner provided the same BPD (e.g. by downloading an entire database onto a drive and giving it to one of the Agencies), no warrant would be required.

iii) The degree of intrusion is identical in both cases, accordingly there is no good reason for the absence of authorisation.

iv) This defect is proposed to be addressed by the Investigatory Powers Bill [A1/17], which will require judicial approval for acquiring BPDs (Part 7, clause 188) and personal approval by the Secretary of State (clause 191).

b) There are no temporal limits on the acquisition or retention of data. In contrast, a warrant (and the information acquired under it) only has a limited period of validity.

c) There is no bar on the transfer of entire Bulk Personal Datasets to other intelligence agencies outside the UK, even where the recipient will not provide adequate protection or safeguards for the security or use of the dataset. No safeguards apply once datasets have been shared.

d) There is no procedure to notify any use or misuse of a Bulk Personal Dataset, so that they can seek an appropriate remedy before the Tribunal.

Issue 4: Necessity and proportionality

83. In light of the findings of the Burnton Report [A4/82], it was neither necessary nor proportionate to collect, retain or use BCD under section 94 TA [A1/1]:

a) The circumstances involve a more comprehensive and intrusive database than any previously considered by the Strasbourg court:

i) A profile is built or capable of being built about any identifiable individual;

ii) The profile will reveal:

a) network of family;

b) friends;

c) business acquaintances;

d) meetings and contacts; and

e) leisure and private activities.

b) A population scale database of such sensitive personal information provided to the Agencies on a blanket basis without Parliamentary, judicial or independent authorisation of access is disproportionate.[6] This is clear from the Strasbourg and Luxembourg case law. See:

i) *MK v France* (Application 19522/09) [A3/56] at §40 "*accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*") applying *S & Marper v UK* [A3/54]. A DNA fingerprint is less intrusive personal information than a detailed record of a person's location and personal associations collected over several months.

ii) The decision in *Digital Rights Ireland* [A3/62] (approved as reflecting ECHR law in *Szabo v Hungary* [A3/61]).

c) Further, the use of section 94 TA data, once acquired, as an unregulated BPD is more intrusive and has fewer safeguards than the RIPA process under Part I, Chapter II [A1/7]. Sir Stanley Burnton found in his July 2016 report [A4/82] at §8.31 that most usage of section 94 data could have been managed satisfactorily under ordinary RIPA procedures.

84. The Claimant may make further submissions on the necessity and proportionality of BPDs once Sir Mark Waller's report is available. But the very fact that BPDs contain intrusive databases of information about mainly innocent people and can be used to

[6] The Claimant reserves its position as to the compatibility of bulk data collection generally with Article 8.

build automated profiles (as with BCD above) makes the collection and retention disproportionate.

F. Conclusions

85. The Tribunal is invited to hold that:

a) the use of section 94 TA to collect BCD is unlawful as a matter of domestic law;

b) the section 94 regime and the BPD regime were and are not in accordance with the law; and

c) both regimes fail to meet a strict test of necessity or proportionality.

86. If the Tribunal accepts the Claimant's submissions, the issue of what remedies (if any) ought to be granted can be determined at the hearing in November 2016.

THOMAS DE LA MARE QC

BEN JAFFEY

DANIEL CASHMAN

Blackstone Chambers

20 July 2016

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

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 SKELETON ARGUMENT

For hearing commencing: Tuesday 26 July 2016

Amended with Bundle References

Privacy International
62 Britton Street
London
EC1M 5UY

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