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

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

CLAIMANT'S SKELETON ARGUMENT
for hearing commencing 17 October 2017

I. INTRODUCTION

1. Four issues are to be determined at this hearing:

   a) the legality of transfer and sharing of BCD and BPD;

   b) the delegation by the Foreign Secretary to GCHQ of the specific requests made under s.94 Telecommunications Act 1984 ('**TA 1984**');

   c) the effect of the finding that the s.94 regime was not 'in accordance with law' on the Respondents' collection of BCD under the extant s.94 directions (up until 13 October 2016); and

   d) proportionality under the ECHR.

   Outstanding issues include the report on searches and proportionality under EU law, which the Tribunal is invited to determine once the CJEU has considered the Tribunal's reference.

2. In summary:

a) There appear to be no adequate safeguards governing the transfer of data from the Agencies to other bodies, whether they are other UK law enforcement agencies, commercial companies or foreign liaison partners.

b) The fact that the s.94 Directions for GCHQ are worded such as to delegate the power to request BCD, and the form of BCD requested, to the Director of GCHQ or any person so authorised by him makes the relevant directions (i) unlawful under domestic law; (ii) in breach of Article 8 ECHR; and (iii) unlawful under EU law.

c) As a result of the Tribunal's judgment reported at [2017] 3 All ER 647 (the '**October Judgment**'), s.94 Directions made before avowal were *ultra vires* and so void *ab initio*. It follows that the Respondents' actions in collecting BCD became lawful not upon avowal, but only upon their collection pursuant to the authority conferred by the revised s.94 Directions issued on 14 October 2016 (after the October Judgment had been provided to the parties in draft).

d) The s.94 regime and the BPD regime are a disproportionate interference with Convention rights.

II. SHARING BPD AND BCD WITH THIRD PARTIES

3. This Tribunal held in its October Judgment at [95], underlining added:

> *The only area in which we need to give further consideration relates to the provisions for safeguards and limitations in the event of transfer by the SIAs to other bodies, such as their foreign partners and UK Law Enforcement Agencies. There are detailed provisions in the Handling Arrangements which would appear to allow for the placing of restrictions in relation to such transfer upon the subsequent use and retention of the data by those parties. It is unclear to us whether such restrictions are in fact placed, and in paragraph 48.2 of their Note of 29 July 2016 the Respondents submit that the Tribunal is not in a position to decide this issue. We would like to do so and invite further submissions.*

4. The issue in *Liberty/Privacy (No. 1)* [2015] 1 Cr App R 24 was the legality of the regime for *receipt* of intercept material collected by foreign partners. This case concerns the reverse situation: what standards and safeguards apply to bulk data which is given to third

parties? Indeed, BPDs may well contain intercept material; it has been avowed that some BPDs are obtained by interception.[1]

A. Facts

5. Before considering the evidence provided by the Respondents on their sharing of BPD and BCD, the Claimant notes that there is a striking omission in the evidence provided by the Respondents, which arises from an artificially narrow (and incorrect in law) definition of 'BPD' having been adopted by the Respondents. This is discussed in legal submissions contained within §§13-21 of the amended fifth witness statement of GCHQ Witness dated 21 June 2017:

a) The Claimant relies upon the definition of a BPD contained within the ISC (Additional Review Functions) (Bulk Personal Datasets) Direction 2015:

> *"any collection of data which … comprises personal data as defined by section 1(1) of the Data Protection Act 1998 … relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest [and] is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies".*

b) It follows, therefore, that a dataset of raw sigint data – provided it meets the above criteria – is a BPD within the meaning of the 2015 Direction.

c) The Respondents, however, have provided their evidence on the basis that a dataset consisting of raw sigint data cannot be a BPD (see §21 of the amended fifth GCHQ witness statement).

d) The Claimant asked, by way of its RFI concerning the fifth witness statement, whether the Respondents' evidence would stand if a BPD were assumed to include a dataset of raw sigint data. The Respondents merely stated that *"it is neither necessary nor appropriate to answer a request on the basis of an incorrect definition"* (responses to Q7 and Q10, 26 July 2017).

e) It follows that the Claimant and the Tribunal are being presented with an incomplete picture of the evidence regarding the transfer of BPDs.

---

1 David Anderson QC, *Bulk Powers Review* (August 2016) fn 119.

12. A specific example of BCD being so transferred in 2010-11 is described as follows (§33(b)): *"One of the databases that the samples were extracted from (REDACTED) was a telephony events database and would have contained at least some s94 data. ... As the samples have since been destroyed at our and the partner's locations we do not have any records of exactly what they included. The data was transferred via an encrypted laptop transported from Benhall to the partner's location via the secure courier service ..."*.

13. It was confirmed in the response to the Claimant's RFI that, in relation to such transfer, *"queries of data not held on GCHQ systems will not be logged by GCHQ"* and the Commissioner *"has not requested to look into the use made of such data in detail"* (response to Q8, RFI of fifth amended witness statement).

14. In terms of remote access by industry partners, the GCHQ Witness confirmed that *"one database containing BPD has been accessed remotely by a small number of individuals (fewer than 20) working for industry partners. ... We cannot demonstrate exactly what data was accessed on these occasions"* (amended fifth witness statement, §29(b)).

15. One important industry partner is the University of Bristol. Snowden documents[4] indicate that researchers are given access to GCHQ's entire raw unselected datasets, including internet usage, telephone calls data, websites visited, file transfers made on the internet and others. Researchers are also given access to GCHQ's entire targeting database (*"delivered... at least once a day..."*), an exceptionally sensitive dataset:[5]

> **F.1.1 SALAMANCA**
>
> *The contents of this dataset are classified* TOP SECRET STRAP2 CHORDAL.
>
> GCHQ collects telephone call record events from a wide variety of sources, and these are stored in a database called SALAMANCA [W36]. This data is also fed to the SUN STORM cloud and the BHDIST DISTILLERY cluster (and other DISTILLERY clusters). This data is a relatively low rate feed of user events, around 5000 events per second, and can be viewed as

[4] These documents are in the public domain and accordingly can be used in these proceedings: R (Bancoult) v Secretary of State for Foreign and Commonwealth Affairs [2013] EWHC 1502 (Admin) at [35]. Where the Claimant refers to a redacted version of such a document, the Tribunal is asked to look in CLOSED at the original and unredacted version of that document.

[5] The extracts below are curtailed at F.1.1, F.1.2 and F.1.4.

F.1.2 FIVE ALIVE

FIVE ALIVE is an ICTR prototype Query Focused Dataset (QFD) providing access to bulk IP-IP connection events, giving a unique unselected view of all activity on SIGINT bearers. Each record in FIVE ALIVE summarises a *flow* between two IP addresses. This summary

F.1.3 HRMap

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL.

When a user requests a webpage from the internet, this is observed in SIGINT as an HTTP GET request. As well as the page requested it often contains the URL of the previously viewed page. The hostname of the requested page is the "HOST" and the hostname of the previous page is the "REFERRER". When we consider just the hostnames rather than the full URI then this is considered events data. This can be viewed as a directed graph of hostnames, and is given the name HRMap at GCHQ. It is a moderately high rate stream (around 20000 events per second) which should be suitable for the streaming EDA and streaming expiring graphs topics.

F.1.4 SKB

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL UKEO.

The Signature Knowledge Base is a system for tracking file transfers made on the internet. A record is made each time we see certain file types being transferred. Each file is identified by its format and a hash of some of its content. Whilst this does mean we can store the data,

F.3.2 Target selectors

The contents of this dataset are classified TOP SECRET STRAP2 UKEO.

Our target knowledge database is BROAD OAK which includes the ability to task various selector types including phone numbers and email addresses. The resulting list of selectors is sometimes called the target dictionary and is delivered to our DISTILLERY clusters at least once a day, and is also available on our Hadoop clusters. This data could be used to see if some result set contains an increased density of targets.

16. The GCHQ Witness states, in relation to GCHQ's partnership with the University of Bristol, that (amended fifth witness statement, §39):

> *"For those researchers who have access to GCHQ operational data, or have done so in the past, the data to which they have access is heavily circumscribed and restricted to what they need for their project. None of this data consists of BPD or BCD, nor has it in the past."*

However, the restrictive definition of a BPD adopted by the GCHQ Witness is likely relevant here.

17. In relation to the Claimant's summary of the partnership (repeated above from an earlier skeleton argument), the GCHQ Witness states that *"[w]e acknowledge that the University of Bristol is an important partner, and that our targeting database is an exceptionally sensitive dataset. The rest ... is untrue"* (amended fifth witness statement, §40). The departure from

the 'NCND' principle is noted. However, it remains unclear what in particular the Respondents say is untrue, or how their position is to be squared with the Snowden documents. When asked in the RFI whether the University of Bristol was given the GCHQ targeting database, the Respondents refused to answer (Q11). The actual position will need to be resolved in closed, with the assistance of Counsel to the Tribunal. The Claimant invites the IPT to make findings of fact that GCHQ's industry partners, including the University of Bristol, have:

a) been given access to highly sensitive material;

b) including (in at least one case) access to GCHQ's targeting database; and

c) no audit records have been maintained of actual access to and use of the material so that the necessity and proportionality of the breaches of privacy involved can be considered by the Tribunal or the Commissioners.

18. There is little, if any, oversight by the Commissioners in respect of either transfer of BCD or BPD or remote access to it. The response from the Commissioners dated 2 June 2017 explained:

> *"Neither Commissioner with responsibility for the intelligence agencies, nor their inspectors, has ever conducted a formal inspection or audit of industry in this regard."*

19. This was confirmed by the response from the Investigatory Powers Commissioner's Office dated 19 September 2017, which explained that there was no audit of industry partner sharing, either before avowal (because it was unknown by the Commissioners) or following avowal (p. 2):

> *"A review of the corporate record of ISCom has established that following the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015 there is no corporate record that the Commissioner audited any sharing of Bulk Personal Data sets (BPD) with UKIC "industry partners" nor is there any material in the corporate record to show that such sharing was considered during an inspection visit of UKIC undertaken by ISCom.*
>
> *A review of the corporate record of the IOCCO can establish that following avowal of the use of Section 94 Telecommunications Act 1984 there is no record that the Commissioner audited any sharing of Bulk Communications Data (BCD) with UKIC "industry partners" nor is there any evidence that such sharing was considered during any inspection visit of the UKIC undertaken by IOCCO.*

Neither ISCom nor IOCCO were previously informed by GCHQ that the sharing of BPD/BCD data sets with industry partners, as described in the statement of the GCHQ witness supplied with the above letter, had occurred."

20. The amended fifth witness statement of GCHQ Witness confirmed that the Commissioners were not briefed about GCHQ's use of industry partners until after this claim had commenced, and only then on an aspect of such sharing (§41):

> *"Sir Mark Waller was specifically briefed in October 2015 and April 2016 on an aspect of [sharing with industry] when it resulted in the activities of industry partners being reflected explicitly in GCHQ's warrantry arrangements ...".*

21. The response from the Investigatory Powers Commissioner's Office dated 19 September 2017 confirmed that the Commissioners first became aware of sharing with industry partners by virtue of the statement of the GCHQ Witness in these proceedings (answer to Q1). On discovering that such sharing took place, the *"IPC immediately ordered that an inspection of those UKIC agencies that may share datasets should be undertaken"* (answer to Q4). However, the Commissioners (now the Commissioner) have still never inspected or audited the procedures and safeguards adopted for sharing with industry partners (answer to Q6), nor the use of such data by industry partners (answer to Q6), nor whether those safeguards are complied with (answer to Q7), nor the use made of shared datasets by industry partners (answer to Q8), nor whether industry partners comply with retention, storage or destruction requirements (answer to Q12).

22. Given these commendably clear and frank answers from the Investigatory Powers Commissioner, it cannot sensibly be suggested that there has been adequate oversight of this activity, sufficient to provide meaningful protection against arbitrary conduct as required by Article 8 ECHR.

Sharing with foreign agencies

23. The Respondents have not maintained a consistent "neither confirm nor deny" position in relation to sharing with foreign agencies. It has been confirmed that at least one communications service provider ('**CSP**') has been sufficiently concerned to demand that foreign sharing of its customers' BCD 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)

24. The Agencies share bulk data with foreign partners, in particular the Five Eyes countries. The pretence of NCND is maintained as to the fact of outward (but not inward) sharing. But this NCND plea is unreal in light of materials now in the public domain. GCHQ disclosed a revised "*GCHQ Policy for Staff from OGDs and SIA partners with access to GCHQ systems and data*" on 11 May 2017. Paragraph 9 avows receipt of "*Sigint and non-Sigint data*" from "*the 5 Eyes partners*" to GCHQ.

25. Moreover, the Five Eyes relationship is governed by the UKUSA agreement. The UKUSA agreement is in the public domain. It explains that Five Eyes is a *reciprocal* sharing partnership. See Article 4 and Appendix C, para. 3 (*"each party will continue to make available to the other continuously, currently, and without request, all raw traffic..."*). It is also avowed that BPD may be obtained by interception (David Anderson QC, *Bulk Powers Review*, footnote 119). Accordingly, it has now been confirmed by official sources that there is sharing of data held in BPDs with the Five Eyes foreign partners.

26. The Snowden documents contain more detail of the types and extent of information sharing that take place, and the risks involved. For example:

a) The Director of the NSA was briefed that Sir Iain Lobban (former Director of GCHQ) was likely to ask about whether UK-sourced data might be given by the NSA to, for example, the Israeli government, to conduct "*lethal operations*". The fact that GCHQ needed to ask such questions indicated that appropriate safeguards were not in place at the time of transfer:

> - (TS//SI//NF) **UK Intelligence Community Oversight**: GCHQ and its sister intelligence agencies are challenged with their activities and operations being subject to increased scrutiny and oversight from their government (and public). As a result, closer attention is being paid to how UK-produced intelligence data is being used by NSA, and other partners. It is possible that Sir Iain may ask about what safeguards NSA may be putting in place to prevent UK data from being provided to others, the Israelis for instance, who might use that intelligence to conduct lethal operations. *For additional information about this subject, and other UK Intelligence Community legal issues and legislation, see the attached paper prepared by Mr.* [redacted]*, Office of the General Council, London.*

b) GCHQ documents confirm that sharing takes place with other Agencies and foreign partners, including data transfers in bulk and remote access. GCHQ

share information under section 19. A bare statutory power to share does not constitute a meaningful safeguard against arbitrary conduct.

b) If a BPD contains intercept material, the basic safeguards in section 15(2) and (3) of RIPA limiting the number of persons to whom the material is disclosed, the extent of copying and arrangements for destruction may be disapplied by the Secretary of State. The Secretary of State may decide to retain such requirements *"to such extent (if any) as the Secretary of State thinks fit"* (section 15(7)(a) of RIPA).

c) Nothing in s.94 TA 1984 imposes any restriction on sharing.

d) The Data Protection Act 1998 ('**DPA**') has been abrogated by ministerial certificate. The eighth data protection principle provides *"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"*. That principle is disapplied by each of the Agencies' certificates made under section 28 of the DPA. For example, GCHQ's certificate 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.

34. Nor is there any secondary legislation or Code of Practice providing safeguards over the sharing of BPD or BCD.

35. There are three reasons why this situation is in breach of Article 8 ECHR:

a) it constitutes a circumvention of the limited safeguards in the TA 1984, RIPA and DRIPA;

b) the absence of foreseeable rules and safeguards; and

c) the inadequacy of those safeguards.

36. A section 94 Direction may be made only if '*necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom*'; on the face of the statute, the BCD direction may be made only for national security/international relations purposes. However, the ability to share data so acquired for other purposes circumvents this restriction:

a) As explained above, neither a body such as HMRC nor the agencies could obtain a section 94 authorisation for a non-national security purpose, such as the detection of tax evasion. Other powers exist to obtain communications data for that purpose, in Part I, Chapter II of RIPA.

b) If GCHQ and/or MI5 give access to their section 94 data to HMRC, for the purposes of detecting tax evasion, HMRC is circumventing the RIPA safeguards. HMRC and the NCA could have requested and obtained communications data themselves under RIPA. The effect of getting access to the same data under section 94 is to circumvent the protection provided by the role of the Designated Person, the Single Point of Conduct, the Interception of Communications Commissioner and the other safeguards in the Codes of Practice.

c) Such circumvention is not compatible with Article 8 ECHR. In *Liberty/Privacy (No. 1)* [2014] UKIPTrib 13_77-H, the Tribunal held that Agencies must apply the RIPA safeguards by analogy when obtaining information from a foreign partner. This was common ground: see [30] and [53]. Where there was no procedure to ensure that RIPA safeguards were always implemented, such a procedure had to be introduced.

37. Moreover, such use also circumvents the safeguards provided by DRIPA and the Regulations made under it, which built upon the basic architecture of RIPA. For instance, such 'recycling' of BCD would enable the Security Services to share data retained by it beyond the 12-month limit applicable to bodies bound by section 1(5) of DRIPA. Such a use, of an obscure and very generally worded power, to circumvent an express statutory safeguard in a regime designed for and addressing the very topic in

hand (data retention for access for subsequent authorised official access to investigate crime) is obviously unlawful.

38. Second, the arrangements are not sufficiently foreseeable. There are no published arrangements governing the safeguards to be applied when considering sharing of data with foreign intelligence services or other UK law enforcement agencies. It was only between March and July 2017 that limited disclosure was given in general terms about the approach of each of the Agencies to sharing. Until the present hearing, such materials have not been in the public domain. Even now, it is unclear what the policy of MI5 and MI6 in fact is. It appears that GCHQ operates a policy requiring that, for remote access, sharing partners adopt a level of protection equivalent to GCHQ's own safeguards (see amended fifth witness statement of the GCHQ Witness at §28). No clear answer has been given to the RFI asking whether MI5 and MI6 operate the same requirements. It appears that they only do so *"insofar as considered appropriate"* (Response to RFI 10 May 2017, paras. 7, 10), which is unilluminating.

39. The Claimant has made further efforts to attempt to discover the outline of the applicable policy. In the Claimant's skeleton for the directions hearing on 5 May 2017 it said:

> *As to sharing, the Claimant's understanding is that GCHQ has an internal policy requiring the recipients of such bulk datasets to have equal safeguards to GCHQ's own safeguards; however, neither MI5 nor MI6 have such a policy, instead operating an entirely discretionary internal process. It is also understood that, unlike the provision under s. 12 of RIPA 2000 or (the broader provision) under s. 171(9) of the Investigatory Powers Act 2016, there is no requirement for the Secretary of State personally to authorise transfer to a body which derogates from the safeguards specified in domestic law. If the Respondents confirm that the Claimant's understanding is correct, the Claimant will not need to request further information on these topics at this stage; and can make substantive submissions accordingly.*

40. The Respondents were ordered to provide a response to this paragraph.[7] The GLD replied on 10 May 2017 indicating that *"the Respondents do not give the confirmation requested"*. The arrangements are therefore still not foreseeable because the actual policy of MI5 and MI6 remains opaque. It is not clear whether:

a) Secretary of State approval is required as indicated above; or

---

7 Paragraph 1(c) of the Tribunal's Order dated 5 May 2017.

b) MI5 and MI6 in fact require equivalent standards when sharing datasets.

41. Finally, the safeguards are inadequate.

42. Two issues arise. First, the Claimant assumes in the absence of a clear response that the policy of MI5 and MI6 does not in fact require equivalence, in contrast to that operated by GCHQ; nor is the approval of the Secretary of State required for any deviation from equivalence. If so, such standards are plainly inadequate to protect against arbitrary conduct. When an entire dataset (mostly consisting of information about people about whom there is no legitimate intelligence interest) is handed over to a commercial, foreign or UK partner (notwithstanding the question of proportionality of such action), it is essential that high standards are applied. If the standards applied are worse than those operated by the agencies (perhaps in terms of oversight, security or the protection of privacy) it is impossible to see how the sharing is lawful.

43. Second, a crucial factor is likely to be the presence or absence of oversight and control:

a) The Commissioners have never carried out an audit of transfer of BPD/BCD.

b) Nor could the Commissioners currently audit the queries of data not held on the SIAs' systems, because they are not logged (see, e.g., response dated 26 July 2017 to Q6(a) of RFI; see also the answer to Q9 in the response from the Investigatory Powers Commissioner's Office dated 19 September 2017). Misuse could not be discovered, and an individual would be unable to make an effective claim to the Tribunal, because the Tribunal's standard searches would fail to detect such misuse.

c) There appears to be no basis for the Agencies to prevent information being used improperly, such as in support of an unlawful rendition operation, mistreatment or torture.

C. EU law

44. The position under EU law for the sharing of BCD is *a fortiori*. As the Tribunal's recent judgment notes, it is the Claimant's position that, to the extent that BCD is transferred out of the EU, this is unlawful following *Watson*: see §§114, 122 and 124.

45. Secondly, it is admitted that s.94 TA 1984 BCD (which can be obtained only for national security purposes) is repurposed for serious crime investigations that do not raise any national security issue: see e.g. third witness statement of GCHQ Witness §§33-37. In these circumstances, BCD is being collected and used for ordinary criminal investigations and the safeguards and standards in *Watson* must apply, even on the Respondents' own case on the scope of EU law.

46. The matter has become yet clearer following the CJEU's judgment in *Opinion 1/15* (ECLI:EU: C:2017:592). The CJEU emphasises repeatedly the purpose to which the data is put as part of the analysis of whether the derogation from Article 8 of the Charter is strictly necessary.

47. The CJEU emphasises repeatedly the need for *"clear and precise rules"* explaining the uses to which the data may be put (at [141]); and thus, at [154]-[163], the CJEU found the draft PNR agreement to be defective in a number of respects in view of the open-ended or vague nature of the language it employed.

48. At [175]-[181], the CJEU considers whether *"the purposes for which PNR data may be processed"* are limited to what is strictly necessary. On the basis that the PNR data *"may be processed by the Canadian Competent Authority only for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime"* ([175]), with the two latter terms being given specific definitions, the CJEU concluded that the agreement *"contains clear and precise rules limited to what is strictly necessary"* ([178]).

49. In contrast, the draft PNR agreement also contained authorisation for Canada to process PNR data *"on a case-by-case basis"* in order to *"ensure the oversight or accountability of the public administration"* and to *"comply with the subpoena or warrant issued, or an order made, by a court"* (at [179]). The CJEU unhesitatingly found this to be unlawful: the provisions were *"too vague and general to meet the requirements as to clarity and precision required"* (at [181]).

50. So, too, a requirement to provide BCD for national security purposes in circumstances where that data may end up being repurposed by tax authorities or by other domestic agencies, with no express statutory authorisation for the sharing of that particular information, would be found to go beyond what was strictly necessary in violation of

Articles 7 and 8 of the Charter. This is *acte éclairé*. The Defendants' favoured tools of recourse to ambiguous general enabling powers that can only leave one speculating as to the potential use made thereof is plainly impermissible under EU law.

III. DELEGATION TO GCHQ OFFICIALS

51. The wording of s.94(1)-(2) of the TA 1984 gives two powers to the Secretary of State:

authorised, provide to GCHQ as requested data generated by or available to [Name of CSP] and associated with communications being or that have been conveyed by means of a Public Telecommunications System (PTS) and data concerning the topology and configuration of [Name of CSP]'s PTS. ...

56. Paragraph 2 of the New Direction provides (emphasis added):

> *[Name of CSP] shall, if requested to do so by the Government Communications Headquarters (GCHQ), acting through the Director of GCHQ or any person authorized by him to make such requests and previously notified to [Name of CSP] as being so authorised, provide to GCHQ communications data (as defined in section 21(4)(a) and (b) of Chapter II of Part I of the Regulation of Investigatory Powers Act 2000) generated by or available to [Name of CSP] in connection with its normal business operations and associated with communications being or that have been conveyed by means of a Public Telecommunications System (PTS). ...*

57. As a matter of domestic law, Parliament has conferred the wide-reaching and highly intrusive powers under s.94 TA 1984 on the Secretary of State. Yet the structure of the Direction is either to delegate to the Director of GCHQ the substance of the function under s.94(1) or, more probably, to delegate to him the power of specific direction under s.94(2).

58. On any view, this delegation under the section 94 Directions entirely circumvents the distinction drawn in the legislation between sub-sections 94(1) and 94(2), being a distinction between directions of a general character and specific directions. The Director of GCHQ (or whoever else is authorised) may be making either a general or a specific direction under the broadly-worded delegation. The legislative purpose in drawing this distinction in the statute is thereby further frustrated.

59. The matter is compounded by the fact that the Old Direction did not even incorporate the formal categories of information of which the Director (or his delegate) may request, thus obscuring the power of *de facto* specific instruction of the kind enabled only by s.94(2). So, on its face, the Old Direction was entirely open-ended. The instruction to a PECN would only be intelligible or complete if the PECN had *both* the Old Direction and the instruction made under it.

60. In delegating this power to the Agencies, the Respondents have thereby frustrated the legislative purpose. The question does not even arise as to whether there is lawful delegation within the Secretary of State's ministerial department for the purposes of the

Carltona principle – the Director of GCHQ is himself constitutionally demarcated from a Secretary of State by section 4 of the Intelligence Services Act 1994 and thus cannot be delegated powers under the *Carltona* doctrine: see *R (Bourgass) v Secretary of State for Justice* [2015] UKSC 54 at [55].

61. In addition to these issues of legality under domestic law, the delegation of the power under section 94 affects the conformity of the section 94 regime with Article 8 ECHR and with rights under the EU Charter. At the July 2016 hearing before the Tribunal, the Respondents relied on the fact that it would be the Secretary of State personally making requests for BCD under section 94 as an important safeguard to the exercise of the power; indeed, the section 94 regime was even contrasted with a power to request data that could be exercised by the Agencies. For example, the Respondents' skeleton argument for the July 2016 hearing contained the following assertions (emphasis added):

> *29. It is all the more plain that that was Parliament's intention when consideration is given to the fact that the exercise of the power is constrained in other ways. Specifically:*
> *... (b) the category of those who can make a direction is extremely limited – directions can only be made by a Secretary of State.*
>
> ...
>
> *40. Secondly, the power to make directions for the production of CD under s.94 and the power to make orders under s.22 of RIPA are properly understood as parallel regimes. The regimes could both lead to the production of CD for use for national security purposes. However, those who can exercise the powers are distinct:*
> *a. A direction under s.94 can only be made by a Secretary of State. A s.94 direction cannot be made in the name of an official.*
> *b. An order under s.22(4) of RIPA, by contrast, can only be made by a 'designated person'. Section 25(1) of RIPA specifies a number of 'relevant public authorities', including the police and the intelligence agencies, and s.25(2) provides that "persons designated for the purposes of this Chapter are the individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this subsection by an order made by the Secretary of State."*
>
> ...
>
> *43. ... (b) To the extent that there is greater specificity of safeguards in the RIPA context, that is explicable by reason of the fact that under that regime directions are made by a large number of different officials in a wide range of different organisations throughout the country. It does not follow that the same system is needed in the s.94 context, where a much smaller number of directions are made and then only by a Secretary of State (ie at the highest level of Government).*

...

49. Secondly, the Claimant's argument again overlooks the fact that there is no overlap between the categories of those who can make the two types of orders. A Secretary of State cannot make an order under RIPA s.22, and the array of law enforcement officers and officials who are 'designated persons' for the purposes of s.22 have no power to make a direction under s.94.

50. Thirdly, it is inherent in the Claimant's argument that there is a simple dichotomy between directions made under s.94 (no safeguards) and those made under RIPA s.22 (detailed safeguards). The fact that s.94 directions are made personally in the name of a Secretary of State is in itself an important safeguard that cannot be replicated in a s.22 direction.

...

79. A direction under s.94(1) can only be given where it "appear[s] 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." Further, the Secretary of State can only give such a direction if "he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct." Thus there are, and at all relevant times have been, safeguards in the form of statutory requirements that the giving of a s.94 direction must be, in the independent judgment of a Secretary of State, both necessary for one of the permitted purposes and proportionate.

...

105. As stated above (at §§79-80 above) in respect of GCHQ, s.94(1) itself contains statutory safeguards requiring that the giving of a s.94 direction be, in the independent judgment of a Secretary of State, both necessary and proportionate. Consultation with the CSP is also required under s.94(1). The Secretary of State will thus be appraised of any material factors, including those relating to necessity and proportionality, which the CSP wishes to bring to his/her attention.

62. Each of these submissions to the Tribunal was materially misleading in light of the form of direction in fact used by GCHQ. The Tribunal gave judgment on the basis of the submissions put to it at the previous hearing: see, for example, the Tribunal's finding that, under section 94, "*the Secretary of State has (after the necessary consultation) considered it necessary (and proportionate) to obtain the data*" (see October Judgment at [54]). The Tribunal's judgment answered the question: "*Is it lawful under domestic law for a Secretary of State to issue directions to telecommunications and internet service providers (PECNs) to supply communications data to the Security Service and to GCHQ and for them to store and examine it?*" (ibid at [22]) and assessed "*the lawfulness of obedience to an intercept warrant under the hand of the Secretary of State*" (ibid at [30]).

63. The Respondents' response is contained in the fourth witness statement of GCHQ Witness at §§7-10. The explanation given for why the GCHQ s.94 Directions are in this form is that *"the CSPs in question have always dealt with a very limited number of individuals within GCHQ"* such that *"[w]hen these directions were first drafted, the view was taken that, because the CSPs had an existing working relationship with these individuals, it would be preferable for the section 94 directions to be triggered by a request from one of them"* (at §8). However, the fact of a pre-existing relationship between GCHQ and the CSPs obviously can have no bearing on the legal requirements of the regime (nor is the reason understood on its own terms – the relevant GCHQ individuals could have informed the CSPs of a direction made by the Secretary of State and delivered it on his behalf).

64. Further, the GCHQ Witness states that, in fact, the relevant *"senior GCHQ officials"* with relationships with the CSPs are in practice not exercising a discretion, but are carrying out the wishes of the Foreign Secretary as expressed to them (§§9-10). However, this assertion that no discretion has *in fact* been exercised says nothing as to the proper objective interpretation of the regime required to determine its legality. There is no doubt that, on the GCHQ s.94 directions as worded, such a discretion could be exercised by a senior GCHQ official. In determining whether the regime is structured lawfully under domestic law, and in determining whether there are sufficient safeguards for ECHR and EU law compliance, the Tribunal therefore needs to consider the wording of the s.94 Directions as made. The form of GCHQ s.94 Direction is, and was, unlawful.

65. Precisely the same reasoning extends to the Defendants' attempts to save the Old Direction which did not incorporate the categories of disclosable data in its body, by reference to the list contained in the submission to the Secretary of State. The fact that such list existed in fact, and the practice of seeking the Secretary of State's consent for its amendment (without amendment of the Direction) is irrelevant to the Direction's legality. A Direction so structured does not comply:

a) with domestic law controls principles of *vires*, since the instructions under the Old Direction not only triggered the commencement of the PECN's obligation but also its scope (thus making the impermissible delegation more complete);

b) the *"in accordance with law"* requirement under Article 8 ECHR, as above; and

c) with the requirement for *"clear and precise"* rules on the scope of disclosure obligations: see *Opinion 1/15* at [141] and [154]-[163].

IV. EFFECT OF FINDING OF ARTICLE 8 BREACH ON EXTANT DIRECTIONS

66. In the October Judgment, the Tribunal found that the section 94 regime was not 'in accordance with law' prior to its avowal in November 2015, and thus was in breach of Article 8 ECHR until avowal. The consequence of the Tribunal's finding is that any section 94 Direction made prior to avowal was unlawful, as it was made in exercise of the unlawful regime, and thus was void *ab initio*. The collection of BCD made under such void section 94 Directions was therefore also without lawful authority.

67. This is merely a statement of administrative law orthodoxy. As summarised in Wade & Forsyth *Administrative Law* (11th ed.) p. 247-248, 254:

> *"An act or order which is* ultra vires *is a nullity, utterly without existence or effect in law. That is the meaning of 'void', the term most commonly used. ...*
>
> *Lord Irvine has said [in* Boddington v British Transport Police*] that when an act or regulation has been pronounced by the court to be unlawful, it 'is then recognised as having no legal effect at all'. This consequence flows from the* ultra vires *principle or 'equally acceptably' from the rule of law. ...*
>
> *The question whether unlawful administrative acts were void or merely voidable became a source of confusion in the period when landmark decisions were revitalising administrative law. Historically there was a sound basis for this distinction. But it is now obsolete, the House of Lords having written its obituary notice decisively."*

This orthodoxy is well-captured in both the reasoning of the majority (Lord Phillips PSC) and Lord Hope DPSC (dissenting) in *Ahmed v HM Treasury (No.2)* [2010] UKSC 5, [2010] 2 AC 534, at 689ff.

68. In respect of the position of the SIAs vis-à-vis the unlawfulness of the Secretary of State's directions, *R (Shoesmith) v OFSTED & ors* [2011] EWCA Civ 642 provides relevant guidance. In that case, the council acted on an (ultra vires) direction by the Secretary of State that the council should appoint a new Director of Children's Services. The majority of the Court of Appeal looked to the knowledge of the council and concluded that the council's act of dismissal was null and void; see Stanley Burnton LJ's recognition at [137] that the relevant public authority *"proceeded on the basis that the direction was lawful and took the risk of its subsequently being held to be void"*. So, too, the SIAs knew that the s.94

regime was unavowed and there was no meaningful independent oversight of the use of the power (no doubt at their insistence) and were equally well aware of the risks this posed in terms of Article 8 compliance. The SIAs took the risk that the s.94 Directions would subsequently be held to be void.

69. Upon receipt of the draft and embargoed October Judgment, the Respondents realised that their existing form of section 94 Direction – the Old Direction – was consequently void and without effect. The Respondents therefore decided to issue new section 94 Directions – in the form of the New Direction – which post-dated avowal of the section 94 regime. This is confirmed by the GCHQ Witness (fourth witness statement at §17):

> *"I would add that an additional reason for re-issuing the directions was to allay any concerns that existing directions were void and/or had no prospective effect as a result of the Tribunal's finding that the section 94 regime was not 'in accordance with the law' prior to avowal in November 2015. We did not consider that there would be any merit in any argument to that effect, but the new directions put the position going forward beyond doubt. I am aware that the Home Office section 94 directions were reissued at this time for this reason."*

70. The consequence is that the date from which the Respondents' demands for BCD could potentially have a legal basis which is 'in accordance with law' begins not from the date of avowal of the section 94 regime; rather, such potential compliance is, at the earliest, when requests for BCD were made under a section 94 Direction that is lawful rather than one which is not void *ab initio*. It follows that 14 October 2016 was the earliest date from which the gathering of BCD pursuant to a s.94 Direction was lawful.

71. The Claimant notes that this issue has important practical consequences. In particular, in relation to remedies, the Respondents are alleging that the illegality was too distant for them to be able to ascertain whether the Claimant's data was unlawfully held and deleted, or whether it was never unlawfully held. This excuse will stand no scrutiny where the illegal activity was happening as recently as October 2016.

V. PROPORTIONALITY UNDER ECHR

A. Bulk Powers Review

72. A useful starting point is David Anderson QC's *Bulk Powers Review* (August 2016), which examined the "*operational case*" for such powers (p. 27). Crucially, Mr Anderson

QC was not permitted to opine on safeguards, nor make any assessment of proportionality (§9.8):

> *"It is not the function of this Report to pronounce on the overall case for bulk powers. The Government has been clear that "consideration of the safeguards that apply to [the bulk] powers, and associated questions of proportionality" should not form part of this Review..."*

73. Mr Anderson QC concluded that there was a good *"operational case"* for BPD and BCD generally, but noted that better oversight was required:

> **"Reducing the privacy footprint**
> *9.23 Also in need of technological expertise are the IPC inspectors whose task it will be to audit the disclosure, retention and use of material acquired pursuant to the new law (clause 205). Are the SIAs' systems equipped with "privacy by design" and if not what can be done about it? Could procedures be amended in such a way as to reduce privacy intrusion (for example by greater use of anonymised search results), without jeopardising operational efficiency? Such issues need a practical understanding of how systems are engineered, how powers are operated, and what could be done to minimise the privacy footprint of the SIAs' activities. The Bill already confers duties to audit, inspect and investigate. What is needed in addition is the expertise to enable those duties to be carried out in the most effective possible way."*

74. The absence of properly resourced technical audit of BCD and BPD demonstrates that there are not sufficient safeguards over the use of such powers, which are therefore both not in accordance with the law, and disproportionate. The following basic questions do not appear to have been considered:

a) How many 'failed searches' take place, where data is accessed but no useful intelligence purpose is served? Have the Commissioners examined the failure rate?

b) Have the Commissioners considered how the 'privacy footprint' of the use of BPD and BCD could be improved, and less data accessed?

c) What technical understanding do the Commissioners and the Tribunal have of the search techniques and other data processing techniques carried out by the partners with whom data is shared? Are the searches and algorithms audited?

d) How are the Respondents' artificial intelligence techniques (including, for example, the use of algorithms, 'machine learning' techniques, data mining techniques and automated decision making) audited, if at all?

e) What examination have the Commissioners made of profiling, where information from multiple datasets is aggregated, in order to build a comprehensive profile about individuals and their activities?

75. These questions are all suitable for being dealt with in OPEN hearings, but, if necessary, the Tribunal should hear evidence and find facts on them in CLOSED. It is striking that, in their evidence, none of the witnesses called by the Agencies has made any attempt to address the proportionality of the use of BPD and BCD or how the privacy consequences of the collection and use of such datasets can be minimised.

B. Article 8 proportionality

76. Of course, an "*operational case*" does not equal proportionality. An excellent "*operational case*" can be made for a mandatory national DNA database, with a sample forcibly taken from every child at birth, or bulk retention of domestic communications content. Such schemes would nevertheless be unlawful:

a) In *S & Marper v UK* (2008), the UK noted that DNA data, which had proven to be of great value, would be deleted if the applicants were successful. Figures were provided (§92). The Court accepted that evidence (§§115-117) but nevertheless held that the retention of data was disproportionate (§§121-122). An "*operational case*" marks the start of an analysis of proportionality, not the end. A DNA fingerprint (which contains no personal information) is simply a unique identifier. It contains less intrusive personal information than a detailed record of a person's location and personal associations collected over several months, contained in BCD or BPD. Even though a sound 'operational case' may have existed, the retention was unlawful.

b) In *MK v France* (Application 19522/09) the Strasbourg Court at §40 again rejected the idea that blanket and indiscriminate retention of data was lawful "*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".

77. The collection of BCD and BPD involves a more comprehensive and intrusive database than any previously considered by the Strasbourg court. A profile is built or capable of being built about any identifiable individual: not least, who the individual is contacting, what websites the individual is visiting, and where the individual is going. The profile will reveal an individual's network of family, friends, business acquaintances, meetings and contacts and leisure and private activities. Accordingly, a scheme involving blanket retention of BCD or entire datasets of BPD, without independent authorisation, notification of usage or appropriate restrictions on scope is unlawful.

THOMAS DE LA MARE QC

BEN JAFFEY QC

DANIEL CASHMAN

Blackstone Chambers

BHATT MURPHY

22 September 2017

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 17 October 2017

Privacy International
62 Britton Street
London
EC1M 5UY

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