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

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

---

**CLAIMANT'S REPLY**
**for hearing commencing 17 October 2017**

---

*Note: This Reply is served in compliance with the deadline of 5pm on 13/10/17. By email timed 4.36pm on 13/10/17, additional documents were disclosed in OPEN. The Claimant has therefore not been able to address the additional disclosure in this Reply, and will request, if necessary, the right to make further written and oral submissions on it.*

## I. Introduction

1. The Respondents' skeleton argument does not engage with the issues of principle underlying the Claimant's challenge.

   1.1. As to sharing, the Respondents' reproduction of its lengthy annex does not address any of the three criticisms set out at paragraph 35 of the Claimant's skeleton argument.

   1.2. As to the delegation to GCHQ officials of the power under s.94, the Respondents do not appear to disagree with the relevant legal principles as set out in the Claimant's skeleton argument. The sole argument on which the Respondents rely is to say that *as a matter of fact* there was not in fact any illegitimate delegation, even though the directions purported to permit this. Such does not address the formal illegality of the directions and the unlawful potential they create for the purported delegate (GCHQ officials) to

exercise powers that cannot lawfully be conferred upon them.

1.3. As to the relevant date for compliance with Article 8 ECHR, the Respondents attempt to draw a distinction between domestic law *vires* and an act of a public authority not being in compliance with Article 8 ECHR. There is no such distinction. The Respondents' reliance on the Tribunal's discretion as to remedy is accordingly irrelevant.

1.4. As to proportionality, the Claimant notes the Respondents' emphasis on David Anderson QC's conclusion that there is an 'operational case' for BPDs: this is a critically different conclusion from a finding of proportionality, and the two should not be elided (see §76 of the Claimant's skeleton argument).

## II. SHARING BPD AND BCD WITH THIRD PARTIES

2. Preliminary question – the meaning of 'Bulk Personal Dataset'. The Respondents now suggest that a dataset of raw sigint data, in circumstances where it satisfies the definition in the 2015 Direction of a bulk personal dataset, is nevertheless not a Bulk Personal Dataset. The reason given is the "*inconvenience*" (Respondents' skeleton, §10) of the result that it may fall under the responsibility of both the Intelligence Service Commissioner and the Interception of Communications Commissioner. (In reality, the narrow definition is applied by the Respondents because it decreases the scope of the issues before the Tribunal.) This is backwards reasoning; the oversight applied (or not applied) cannot determine whether a dataset does or does not satisfy a statutory definition. Nor can the Respondents' dubious and hitherto secret interpretation of the Direction determine the scope of the complaints made by the Claimants, which (for, the avoidance of doubt, *includes* a bulk dataset of raw sigint data). It is also now irrelevant reasoning, given the combined single role of the Investigatory Powers Commissioner.

3. Alleged safeguards. As to the alleged safeguards which *would be applicable were sharing to occur*, the Respondents summarise the safeguards on which they rely at §§29-32 of their skeleton. Notably, this has provided no answer to the criticisms contained at §§38-40 of the Claimant's skeleton argument: it remains unclear in various respects what the policy of MI5 and MI6 in fact is; and the limited disclosure on which the Respondents rely has not been in the public domain until the present hearing. The only matter that is clear is that, whereas GCHQ will only share where equivalent safeguards are in place, MI5 and MI6 may share

entire datasets without equivalent safeguards being in place. In these circumstances, the rules governing sharing are neither sufficiently foreseeable nor do they provide adequate protection against arbitrary conduct.

4. Commissioner oversight. At §36 of the Respondents' skeleton argument, it is said that sharing *would be* under the Commissioners' (now the Commissioner's) remit. However, the sole example where the Respondents do not maintain NCND, namely GCHQ's sharing with industry, demonstrates that this oversight (while technically within remit) has been, in practice, absent. The Commissioners did not know the sharing was taking place until this claim had been brought. The Commissioners did not, and have not, audited the sharing that was taking place. Nor could the Commissioners currently audit the queries of data not held on the SIAs' systems, because they are not logged.

5. The Respondents' response to this criticism is to say that there has been "*extremely limited*" sharing with industry by GCHQ and therefore actual oversight was unnecessary (Respondents' skeleton, §§55, 57). However:

   5.1. On learning of the sharing, the Commissioner immediately directed that an audit take place. This is inconsistent with the suggestion that no actual oversight was necessary. In circumstances where the Commissioner thought an audit was needed, it is difficult to see how the Respondents can sensibly argue it was unnecessary.

   5.2. The Commissioner appears unable to confirm the extent of the sharing that has taken place. The Commissioner's response dated 19 September 2017 refers to "*apparently very limited*" sharing (emphasis added).

   5.3. The Respondents maintain NCND as to the activity of, and amount of, industry sharing that occurs with MI5 and MI6, yet also seek to maintain that the lack of Commissioner oversight would not matter because the sharing that happens by GCHQ is limited. The situation may very well be different for MI5 and MI6 – the Claimant has no means of testing this argument.

   5.4. It is in any event denied that it is a valid argument to rely on the fact that such sharing has been limited. The potential and capacity for abuse is vast, yet this activity went unnoticed and unchecked for many years; it would likely still be so were it not for this

claim.

5.5. Significant aspects remain to be inspected or audited: see §21 of the Claimant's skeleton argument. Indeed, although the Commissioner has carried out an inspection, the results of the inspection have not been disclosed. Actual auditing is presently not possible because queries of data not held on GCHQ systems will not be logged by GCHQ: see §13 of Claimant's skeleton argument. The Commissioner also appears to consider that he has no right to audit the Companies directly; the audit provisions of the relevant contracts have not been disclosed, and so the Claimant is unable to comment on whether this position is correct, but it appears to be a significant lacuna in oversight.[1]

6. Sharing with law enforcement partners. The Respondents deny that there would be any circumvention by, for example, sharing s. 94 BCD with HMRC, in circumstances where it would otherwise need to comply with RIPA safeguards to obtain such information. The Respondents rely on s.19 of the CTA, suggesting that this would authorise such disclosure.

7. However, the Respondents' argument fails to engage with the question of why, in that case, s. 94 TA 1984 restricts a Direction to being made only if *"necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom"*. These statutory words must mean something. The Respondents' interpretation circumvents the very restriction built into s. 94, and also circumvents the safeguards that would normally apply for law enforcement to obtain the same communications data under RIPA. Even as a matter of domestic law, a generally-worded provision creating a special rule (s.94, which is a departure from an otherwise comprehensive regime in RIPA) enabling compelled disclosure of BCD for a narrow, defined purpose, namely national security, cannot lawfully then be broadened with a general power of disclosure as to defeat the detailed statutory safeguards designed to prevent disclosure of BCD to all other public bodies save in defined circumstances. For s.19 CTA be used in such a way, unless the conditions of RIPA are also met in the case in hand, is to use such powers for a *Padfield* improper purpose or otherwise *ultra vires*.

8. The same conclusion flows as matter of EU law:

[1] The Claimant raised this point with Counsel to the Tribunal. By email dated 13 October 2017, the Respondents stated that they were *"making enquiries"* and *"hope to be able to provide information in this regard early next week"*.

8.1. The Respondents specifically accept that the purpose for which information would be disclosed under such a programme would be *"supporting the prevention or detection of serious crime"* (§47). At this point, the Respondents' argument as to the scope of EU law falls away, as it is not a matter of *"national security"*. It does not appear to be in dispute that, were the PECNs providing BCD to HMRC directly, EU law would be engaged and the *Watson* safeguards would be applicable. The Respondents' argument (§61.2) is that the fact of one of the SIAs acting as an intermediary takes the matter outside the scope of EU law and renders the *Watson* safeguards inapplicable. Such a formalistic argument is untenable under EU law, and is expressly addressed and prohibited by *Opinion 1/15*: see §§88, 125 and 212-215. EU law is engaged, and the safeguards under the Charter are applicable, because BCD is being taken from PECNs and is being given to HMRC – the precise way in which this occurs (whether direct or indirect) is not capable of rendering the privacy concerns under the Charter inapplicable.

8.2. Nor does the statutory regime provide *"clear and precise rules as to the purposes for which such BCD may be used"* (Respondents' skeleton, §61.2.3). Stating that data may be disclosed for the purpose of *"the proper discharge of [GCHQ's] functions"* or *"any criminal proceedings"* (s.19(5) CTA) is precisely the sort of vague language rejected by the CJEU in *Opinion 1/15* (see §§48-50 of the Claimant's skeleton argument).

9. For all the above reasons, the Respondents' skeleton argument provides no answer to the Claimant's criticism that the present regime regarding sharing of BPD and BCD is in breach of Article 8 ECHR. Nor do these questions need to await the response to the reference. *Opinion 1/15* could not be clearer; and no question of national security exclusive competence arises.

## III. DELEGATION TO GCHQ OFFICIALS

10. The Respondents' analysis is brief (§§62-68). The only point taken is that *in fact* GCHQ officials have not been exercising an independent discretion in selecting and requesting BCD under s.94 Directions. They make no argument to suggest that, in principle, the current formulation of the s.94 Directions is lawful, or that it would be permissible for GCHQ officials to exercise the sort of discretion that is purportedly afforded to them under those Directions.

11. Therefore, the Respondents appear to admit that the past and current form of the current s.94 Directions is unlawful. That is dispostive of its unlawfulness, both in domestic law and under the Convention for the purpose of the "in accordance with law" criterion. In those circumstances, the form needs to match that substance. What the Secretary of State and the Security Services have been doing in practice is potentially relevant only to the scope of any private law damages remedy: see *R(Lumba) v SSHD* [2011] UKSC 12; [2012] 1 AC 245.

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

12. In an earlier skeleton argument, the Respondents had suggested that the resolution of this matter would involve consideration of *"detailed questions of both law and fact"* (§11 of Respondents' skeleton argument for Directions Hearing on 5 May 2017), which was understood to refer to the developing law on void and voidable administrative acts. Instead, the Respondents now rely on (i) an alleged distinction between a direct *vires* challenge to s.94 Directions and a finding that the regime operated by the Respondents was in breach of Article 8 ECHR; and (ii) the fact that the Tribunal has a discretion as to remedy (§77).

13. The first argument is wrong as a matter of law: there is no such distinction.

14. The Respondents' argument seems very largely to hang upon the invocation of the difference in the wording between Issue 1 and Issue 2 as framed before this Tribunal at the first substantive hearing. This a strange argument to advance for anyone with even passing familiarity with the issues (and a sign of the weakness of the Respondents' position). As the Tribunal will remember:

    14.1. Issue 1 approached the question of *vires* as a simple question of domestic law, on the basis that s.94 TA 1984 had to be narrowly construed (using domestic canons of construction) as not extending to BCD because of its legislative history and its interaction with the dedicated and ostensibly comprehensive domestic regime in RIPA, which was applicable to the compelled disclosure of BCD. It was thus recurrently referred to as the point of "pure domestic vires".

    14.2. Issue 2 considered the problem from the different 'external' perspective of Article 8 ECHR and the HRA and, in particular, the requirement for a regime to be "in accordance with law". Any domestic regime that fails (as this regime did, prior to

avowal) to meet that substantive ECHR test is also unlawful. Pursuant to s.6(1) of the Human Rights Act 1998, "*it is unlawful for a public authority to act in a way which is incompatible with a Convention right*". Prior to avowal, the entirely secret *use* of the s.94 regime *to obtain BCD* ("a s.94 BCD Direction") was incompatible with Article 8 ECHR as it was not "in accordance with law". Other avowed uses of s.94, for instance to require (generally) BT to install secure lines, were not unlawful. Whilst the issue was directed at "the s.94 regime" that was no more than a reflection of the fact that the criticised generality or opaqueness of the use of s.94 began with that section's general or oblique wording. But the context of the criticism of the regime was at all times clear, as was the result: it was only the use of s.94 to make *particular types of highly invasive direction* that was unlawful under the HRA, until such use was avowed in general terms and controlled by the use of appropriate guidance. It follows that there were no domestic law *vires* for the making of such s.94 BCD Directions until avowal.

15. Once this is understood, the argument as to discretionary remedy falls away. The Tribunal must apply the logic of its legal findings to the Directions as it finds them, the detail of which was not before it (for reasons entirely unexplained) when it reached its first ruling in the October Judgment. The principled application of that first ruling is clear. Those s.94 BCD Directions which were made before avowal were void *ab initio*, and such initial illegality/voidness does not vanish and is not cured by avowal. The Tribunal does not have the discretion to declare as lawful those acts (the making of s.94 BCD Directions) which it finds, on an application of the relevant and undisputed principles of law, to be unlawful until avowed.

16. It follows that 14 October 2016 (that being the date of the first Directions after avowal) was the earliest date from which the gathering of BCD pursuant to a s.94 Direction could have been lawful.

## V. PROPORTIONALITY

17. An 'operational case' case be made for much conduct which is a disproportionate interference with fundamental rights. A recent example in the ECtHR is *S & Marper*. When considering proportionality, it is necessary to examine whether in fact all that can reasonably be done to minimise the intrusion into privacy of the use of BPDs has been

achieved. As Mr Anderson QC noted, there has never been any assessment of how the 'privacy footprint' of the use of BPD and BCD could be reduced:

> ***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"*,[258] 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.

18. Any assessment of the proportionality of the use of BPDs requires such an analysis. The types of questions that need to be considered are set out in Mr Anderson QC's report and the Claimant's skeleton argument. Answering those questions requires a full understanding of the operation of large scale databases and designing algorithms and queries to minimise intrusions into privacy. Without such an assessment, the true position is that the Tribunal simply does not know whether conduct is proportionate in the sense of being no more intrusive than strictly necessary.

**THOMAS DE LA MARE QC**

**BEN JAFFEY QC**

**DANIEL CASHMAN**

**Blackstone Chambers**

**BHATT MURPHY**

**13 October 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**
10 Tyssen Street
Dalston
London E8 2FE
DX 46806 Dalston