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 REQUEST FOR FURTHER INFORMATION AND DISCLOSURE CONCERNING THE RESPONDENTS' EVIDENCE ON SHARING AND EU LAW

The Claimant requests the following further information and disclosure in respect of the Respondents' Open Evidence received on Friday 10 February 2017 and on the issues of EU law.

The three witness statements and two exhibits raise overlapping issues. Each request should be treated as being made in respect of the activities of each of the three agencies.

GCHQ Witness statement, paragraph 5 (*"this statement … does not address situations which might arise were foreign liaison partners able to use/access GCHQ systems in order to run their own targeted queries against repositories holding BPDs and BCDs"*):

Exhibit GCHQ 3 (*"The Agencies may share applications (which in turn could provide access to another Agency's BPD holdings) as judged appropriate in line with SIA information policy on commissioning"*) and Exhibit MI5 2 (*"Sharing data and applications in-situ* [REDACTION] *Sharing data in this way requires both the requesting and disclosing agencies to assess the necessity and proportionality of the access and use being sought* [REDACTION]")

1. In what circumstances are liaison partners and/or law enforcement agencies (together 'third parties') given remote access to run queries (also referred to as 'share applications' or 'applications in-situ') to SIA datasets?

a) What policies and safeguards apply to the grant of such access? Please disclose them.

b) What safeguards protect legally privileged material in BCD and BPD to which overseas partners and/or law enforcement agencies are given remote access?

c) What safeguards protect journalistic material in BCD and BPD to which overseas partners and/or law enforcement agencies are given remote access?

d) What steps are taken to make the use in fact made by third parties of the access facility auditable? Please disclose them.

e) Has such access ever been misused? What steps were taken in consequence? How was the misuse detected?

f) To what extent do the safeguards governing such access differ from those applying to Agency staff?

g) What controls or safeguards are applied to the retention and use of material obtained by third parties through access? Please disclose them.

2. Have the Commissioners or any other oversight body ever conducted an audit (or similar form of oversight) of the circumstances in which overseas partners and law enforcement agencies have been granted remote access to SIA datasets, the adequacy of the safeguards in place, the compliance with those safeguards, conditions of use and retention and the actual use made of such access?

3. If so, when and how was the audit conducted? What were the results of that audit?

SIS witness statement dated 8 February 2017, paragraph 5:

[*Sharing BCD and/or BPD with non-SIA third parties*]

4. How many times have BCD and/or BPD been shared with non-SIA third parties (e.g. HMRC)?

a) Which categories of BPD and/or BCD have been shared?

b) What restrictions apply to the uses to which BPD and/or BCD obtained from the Agencies may be put?

c) What safeguards are in place in respect of legally privileged material disclosed to non-SIA third parties?

d) What safeguards are in place in respect of journalistic material disclosed to non-SIA third parites?

e) Can BCD obtained for the purposes of protecting national security be re-used by a non-SIA third party for other purposes, including the investigation of crime?

5. If BCD or BPD containing intercept material or communications data is shared, does the non-SIA third party (i) obtain a warrant or authorisation for access under RIPA; and/or (ii) comply with the legal standards that would apply if it had obtained such information itself, directly?

6. Have any of the above safeguards ever been breached? What steps were taken in consequence? How was the breach detected?

7. What oversight have the Commissioners carried out of the sharing of such BCD or BPD and the use to which the non-SIA third party has made of the transferred data?

8. Does the Commissioner audit the use, retention, storage and deletion of the data by non-SIA third parties? Is such use of data auditable and audited? If so, how?

SIS witness statement dated 8 February 2017, paragraphs 9 and 10; GCHQ witness statement dated 9 February 2017, paragraphs 6 and 7; and MI5 witness statement dated 10 February 2017, paragraphs 7-10:

[*Sharing BPD and/or BCD with overseas partners, law enforcement agencies and industry partners*]

9. What assurances are obtained from partner agencies as to the uses to which BPD and/or BCD will be put and the relevant controls that will be applied to retention, use, examination, storage and destruction?

10. In what circumstances is BCD/BPD shared with industry partners, and what controls are applied to retention, use, examination, storage and destruction?

    a) Where BCD/BPD is shared with industry partners, are they required to store it within the EU?

    b) Are industry partners given remote access to BCD/BPD datasets, and if so in what circumstances? What safeguards apply to such acess?

11. Do assurances obtained from overseas partners, law enforcement agencies and industry partners always guarantee the same standards as would be applied by staff of the Agencies?

12. Is an assurance to agree to cease to use transferred data and destroy it on request obtained?

13. Have assurances been breached? If so, when and in what circumstances? How was the breach discovered? What action was taken in response?

14. What oversight have the Commissioners carried out of the sharing of BCD and/or BPD and the use to which overseas partners, law enforcement agencies and/or industry partners have made of the transferred data?

15. Has the Intelligence Services Commissioner or any other oversight body ever audited the sharing of BCD and/or BPD with overseas partners, law enforcement agencies and/or industry partners?

    a) If so, how was the audit conducted?

    b) What were the results of that audit?

    c) Did the audit examine the actual queries and use made of transferred data, and its storage and destruction?

16. What safeguards are in place to protect legally privileged material in BCD/BPD shared with international partners, law enforcement agencies and industry partners?

17. What safeguards are in place to protect journalistic material in BCD/BPD shared with international partners, law enforcement agencies and industry partners?

Exhibit MI5 2, page 12 (section heading: "*4.4 Authorisation of Disclosure*")

18. How many requests have been made to the Home Secretary or a Senior Official in the Home Office for disclosure of an entire BCD or a subset outside MI5?

19. How many of those requests have been approved, and how many rejected?

20. Are these requests subject to the oversight of the Intelligence Services Commissioner or of any other body? If so, how is such oversight effected?

EU law

21. Please disclose a representative sample of BCD notices made under section 94 TA 1984, redacted insofar as necessary to protect national security.

22. Has all BCD been retained in the EU? Has any BCD been shared or held outside of the EU? If so, where and when?

23. What arrangements are in place for the prior independent or judicial authorisation of access to BCD?

24. Is the use of BCD limited to the prevention and detection of serious crime?

25. What arrangements are in place to ensure notification to persons whose data obtained under section 94 has been accessed?

26. Is there general and indiscriminate retention of BCD, within the meaning of the judgment in *Watson*? If not, on what basis is the treatment of BCD said to fall outside this definition?

NCND

27. The invocation by the intelligence agencies of NCND in relation to the fact of BCD and BPD sharing with overseas partners is absurd. There is official information in the public domain confirming the intelligence sharing relationship which the agencies enjoy with (at the very least) the members of the Five Eyes. For example, the IOCCO annual report for 2015 refers to "*sharing of intercepted material and related communications data with foreign partners*" (at [6.83]). The 2015 Annual Report of the Intelligence Services Commissioner repeatedly refers to sharing with "*foreign liaison services.*" In these circumstances, continued reliance by the agencies on NCND is inappropriate. In light of the foregoing, if NCND is to be maintained, what is basis for maintaining this position?

THOMAS DE LA MARE QC
BEN JAFFEY QC
DANIEL CASHMAN

Blackstone Chambers

17 February 2017