Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

RE-RE-AMENDED OPEN RESPONSE OF THE RESPONDENTS TO THE CLAIMANTS' REQUEST FOR FURTHER INFORMATION AND DISCLOSURE DATED 17 FEBRUARY 2017

The Claimant's requests are reproduced below. The Respondents' responses are in bold. As requested, responses are given on behalf of each of the SIAs even where a request relates in terms to only one of the SIAs.

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 even 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.

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

For reasons already stated, the Respondents are unable to confirm or deny in OPEN whether foreign liaison partners or domestic law enforcement agencies have ever been given remote access to SIA systems to enable them to run queries on such systems holding either BPD or BCD. For the avoidance of doubt, this information has been provided to the Tribunal in CLOSED. What the Respondents can say is that were such access to be granted, safeguards would be put in place that would (a) follow the principles and approach set out in SIA Handling Arrangements and policy/guidance (including where appropriate the policies relating to sensitive datasets); (b) take into account the nature of the BPD / BCD to which access was being provided; and (c) take into account the nature / remit of the body that was being granted remote access. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument.

See further paragraphs 6 to 8 of GCHQ's Amended Witness Statement dated 6 March 2017.

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?

~~**The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.**~~

The Intelligence Services Commissioner and Interception of Communications Commissioner have oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD compliance (as applicable), including that relating to providing remote access to third parties to run queries, *were it to occur.*

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

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

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 parties?
   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?

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

For reasons already stated, the Respondents are unable to confirm or deny in OPEN whether they have shared BCD or BPD with foreign liaison partners or domestic law enforcement agencies. For the avoidance of doubt, this information has been provided to the Tribunal in CLOSED. What the Respondents can say is that were such sharing to take place, safeguards would be put in place that would (a) follow the principles and approach set out in SIA Handling Arrangements and policy/guidance (including where appropriate the policies relating to sensitive datasets); (b) take into account the nature of the BPD / BCD that was due to be shared; and (c) take into account the nature / remit of the body with which the data was being shared. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument. See further:

- paragraphs 9 to 14 of GCHQ's Amended Witness Statement dated 6 March 2017;
- paragraphs 5 to 10 of the Security Service's Witness Statement dated 10 February 2017; and
- paragraphs 5 to 24 of SIS's Amended Witness Statement dated 3 March 2017.

The relevant restrictions and safeguards would include the Action-On process. The Action On policy is a broader SIA policy. Insofar as relevant to this case, Action On would allow for the imposition of certain conditions on a recipient of BPD/BCD from one of the SIA, and require the recipient to revert to the sharing SIA before carrying out certain specified activity, such as sharing it further. Were BPD/BCD to be shared, an Action On condition requiring the recipient to revert to the sharing SIA before further sharing or any onward disclosure of the BPD/BCD would be imposed. The recipient would therefore have to revert to the SIA that shared the BPD/BCD if it wished to take such a step to obtain permission to use that BPD/BCD in a way that was not otherwise agreed at the time of sharing. While it is not possible to be categorical that Action On conditions are complied with in every case, the mutual dependence on the process by intelligence and security agencies should lead to a high level of compliance. See further SIS WS paragraphs 21-23 and GCHQ WS paragraph 9.

As to request 4(e), this is a matter of law and thus for submissions.

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

The Respondents cannot respond fully to this request in OPEN as to do so would be damaging to the interests of national security. However, see response to request 4 above.

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

The Respondents cannot respond fully to this request in OPEN as to do so would be damaging to the interests of national security. However, in the event that any of the SIAs' policies and safeguards in respect of sharing BPD/BCD were breached, the relevant Agency would report any such breach to the Intelligence Services Commissioner or Interception of Communications Commissioner (as appropriate); investigate the breach; consider whether it remained lawful or appropriate to continue to share; if and to the extent that any Agency staff had committed the breach in question, consideration would be given to disciplinary proceedings.

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?

The Intelligence Services Commissioner and Interception of Communications Commissioner have oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD ~~governance~~ compliance (as applicable), including that relating to sharing, were it to occur.

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?

See response to request 7 above.

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?

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

For reasons already stated, the Respondents are unable to confirm or deny in OPEN whether they have shared BCD or BPD with foreign liaison partners or domestic law enforcement agencies. For the avoidance of doubt, this information has been provided to the Tribunal in CLOSED. What the Respondents can say is that were such sharing to take place, safeguards would be put in place that would (a) follow the principles and approach set out in SIA Handling Arrangements and policy/guidance (including where appropriate the policies relating to sensitive datasets); (b) take into account the nature of the BPD / BCD that was due to be shared; and (c) take into account the nature / remit of the body with which the data was being shared. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument. See further:

- **paragraphs 9 to 14 of GCHQ's Amended Witness Statement dated 6 March 2017;**

- paragraphs 5 to 10 of the Security Service's Witness Statement dated 10 February 2017; and
- paragraphs 5 to 24 of SIS's Amended Witness Statement dated 3 March 2017.

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

~~This request is still under consideration.~~

The position regarding GCHQ is that BCD/BPD may be shared with industry partners where necessary for the purposes of developing and testing GCHQ's operational systems. Industry partners are required to specify the controls that they intend to apply in relation to retention, use, examination and destruction. These controls are subject to approval before sharing. The approval process is set out in a request form. See further paragraphs 10 to 12 of GCHQ's Amended Witness Statement dated 6 March 2017 and Exhibit GCHQ3.

SIS and MI5 are unable to confirm or deny in OPEN whether they share BPD and/or (in the case of MI5) BCD with industry partners, because to do so would be damaging to the interests of national security. For the avoidance of doubt, this information has been provided to the Tribunal in CLOSED. What the SIS and MI5 can say is that were such sharing to take place, safeguards would be put in place that would (a) follow the principles and approach set out in SIA Handling Arrangements and policy/guidance (including where appropriate the policies relating to sensitive datasets); (b) take into account the nature of the BPD / BCD that was due to be shared; and (c) take into account the nature / remit of the industry partner with which the data was being shared. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument. See further:

- paragraphs 5 to 10 of the Security Service's Witness Statement dated 10 February 2017; and
- paragraphs 5 to 24 of SIS's Amended Witness Statement dated 3 March 2017.

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

~~This request is still under consideration.~~

The position regarding GCHQ is that when operational data (which could in theory include BCD/BPD) is shared with industry partners, it is usually retained within GCHQ premises in the UK. When it is not stored within GCHQ premises, the storage will be accredited by GCHQ. In all such cases the storage has been within the UK.

As regards SIS and MI5, please see the response given above.

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

~~This request is still under consideration.~~

As regards GCHQ, the answer is no. As regards SIS and MI5, please see the response given above.

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?

~~This request is still under consideration.~~

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

~~The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.~~

As regards GCHQ sharing with industry partners, the answer to Requests 11 and 12 is yes.

Otherwise, as previously stated, the Respondents are unable to confirm or deny in OPEN whether sharing of this nature takes place, and it follows that they cannot confirm or deny in OPEN the contents of any assurances that may have been obtained in support of any such sharing (although for the avoidance of doubt this information has been provided to the Tribunal in CLOSED). What the Respondents can say is that were such sharing to take place, safeguards would be put in place that would (a) follow the principles and approach set out in SIA Handling Arrangements and policy/guidance (including where appropriate the policies relating to sensitive datasets); (b) take into account the nature of the BPD / BCD that was due to be shared; and (c) take into account the nature / remit of the organisation with which the data was being shared. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument. See further:

- paragraphs 9 to 14 of GCHQ's Amended Witness Statement dated 6 March 2017;
- paragraphs 5 to 10 of the Security Service's Witness Statement dated 10 February 2017; and
- paragraphs 5 to 24 of SIS's Amended Witness Statement dated 3 March 2017.

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

As regards GCHQ sharing with industry partners, the answer is no.

Otherwise, see the response to request 6 above. ~~the Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.~~

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?

The Intelligence Services Commissioner and Interception of Communications Commissioner have oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD ~~governance~~ compliance (as applicable), including that relating to sharing, were it to occur.

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?

See response to request 14 above.

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

~~This request is still under consideration.~~

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

~~**This request is still under consideration.**~~

In response to Requests 16 and 17, as has been stated above, were sharing to take place, safeguards would be put in place that would follow the principles and approach set out in SIA Handling Arrangements and policy/guidance. A detailed list of relevant policy documents / forms etc (which have already been disclosed in these proceedings) will be set out in the Respondents' skeleton argument. Of particular relevance in this regard would be the terms of the February 2015 joint SIA BPD Policy which states that *"Agencies must protect sensitive datasets (or certain fields within a dataset) when sharing, if the risk of intrusion in doing so is not judged to be necessary or proportionate"*. See also:

- **GCHQ's BPDAR form which requires identification of whether the BPD contains any sensitive personal data, and if so what kind. For the avoidance of doubt "sensitive personal data" is understood to include legally privileged material and confidential journalistic data;**
- **GCHQ's Compliance Guide, which makes clear that particular consideration should be given in cases where confidential information (which includes, inter alia, material that is legally privileged, and confidential journalistic information) is involved. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of such material is necessary and proportionate. This covers any sharing of such data with partners. Any sharing of BPD in whole or in part is subject to formal approval by Deputy Director Mission Policy who will take into account the potential for such data to contain confidential information and ensure that this is removed from the data to the extent possible (e.g. by the removal of particular fields from datasets) and will require the application of additional or more stringent safeguards where appropriate.**
- **The Security Service's *relevant form*, which contains, *inter alia*, provision for considering whether the BPD contains sensitive personal data, including but not restricted to journalistic and legally privileged material;**
- **SIS's BPD Handling Arrangements, §§1.1.7-1.1.8, which require that "Sensitive Personal Data" (defined as including, inter alia, legally privileged material) be subject to greater scrutiny prior to authorisation for exploitation and therefore prior to any disclosure.**

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?

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

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

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

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?

See response to request 14 above. If such requests were made, they would be subject to the oversight of the Interception of Communications Commissioner.

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.

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

Consideration is being given to disclosing in OPEN a suitably redacted representative s.94 notice.

A representative sample of s.94 directions has been disclosed.

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?

The Respondents cannot respond to this request in OPEN as to do so would be damaging to the interests of national security.

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

There are no such arrangements.

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

~~**This request is still under consideration.**~~

MI5's use of BCD has been almost exclusively for national security purposes. However, there have been a very limited number of exceptional cases when BCD has been used for the purpose of prevention and detection of serious crime.

GCHQ's use of BCD is predominantly in the interests of national security, but has included the purpose of 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?

There are no such arrangements.

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?

This request is properly a matter for submissions.

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 NCND is inappropriate. In light of the foregoing, if NCND is to be maintained, what is the basis for maintaining this position?

This request is properly a matter for submissions.

~~**27 February 2017**~~

~~**1 March 2017**~~

~~**6 March 2017**~~

28 April 2017

ANDREW O'CONNOR QC
RICHARD O'BRIEN