

\*Gists are underlined  
Amendments are highlighted

Witness: SIS Witness  
Party: 5<sup>th</sup> Respondent  
Number: 5  
Exhibit: SIS exhibit  
Date: 24.11.2017

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 COMMUNICATION HEADQUARTERS
- (4) SECURITY SERVICE
- (5) SECRET INTELLIGENCE SERVICE

Respondents

---

---

AMENDED WITNESS STATEMENT OF SIS WITNESS

---

---

I, SIS witness, of the Secret Intelligence Service (SIS), Vauxhall Cross, London, SE1, will say as follows:

1. This is an OPEN version of a fuller CLOSED witness statement that I have prepared and bears today's date. I have identified where material that appears in the CLOSED statement has been redacted from this version. Some of the CLOSED content appears in this statement in a gisted form – those gists are underlined.
2. I refer to paragraph 1 of my witness statement dated 8 February 2017 for details of my role within SIS.
3. I am authorised to make this witness statement on behalf of SIS. The contents of this statement are within my own knowledge and are true to the best of my knowledge and

belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within SIS.

4. Further to my previous Witness Statements dated 8 July 2016 (Amended) and 8 February 2017, I make this statement to respond to a number of points that have arisen recently in correspondence between the Tribunal and the Investigatory Powers Commissioner's Office ('IPCO') and that arose at the OPEN hearing during 15 – 17 October 2017. The particular issues are as follows:
  - (i) Types of BPD acquired and used by SIS;
  - (ii) The capabilities and techniques (including "artificial intelligence") that SIS employ in relation to its use of BPD;
  - (iii) The way in which the Commissioner has exercised his oversight of BPD use (including "dip-testing" or "random audit");
  - (iv) The way in which SIS would record and retain action-on requests from foreign partners in respect of BPD if it were to be shared;

#### *Types of BPD*

5. During the OPEN hearing on 17/10/17 (transcript 1/54), Counsel for the Claimant referenced during his submissions that the SIA could hold a social media dataset like "for example, of everybody's Facebook account". I am unable to confirm or deny whether or not SIS holds (in whole or in part) copies of global social media networks e.g. Facebook, Twitter, LinkedIn or Instagram.
6. In paragraphs 10 - 14 of my amended statement of 8 July 2016, I set out the types of BPD holdings that SIS have, from where they are sourced and how they are categorised internally. In paragraph 18 of that statement, I made clear that SIS only acquire and retain BPDs where it is deemed necessary and proportionate for the purposes of carrying out their statutory functions. In assessing the proportionality of SIS's use of BPD, the Tribunal may consider it helpful to understand in more detail the nature of SIS's BPD holdings.
7. SIS acquire datasets which can be used to assist in answering Intelligence questions regarding the intentions or activities of those posing a threat to UK national security, engaged in serious crime or which affect the economic wellbeing of the UK. As a result,

the vast majority of datasets relate directly to non-British nationals. The majority of individuals within datasets to whom the data relates will be foreign nationals.

8. SIS hold travel data

[REDACTED]

9. SIS hold biographical, communications and financial data.

*“Artificial Intelligence”*

10. In its response email of 10 October to the Tribunal’s letter of 2 October 2017, IPCO address a number of questions derived from the Claimant’s skeleton argument. One such question is *“how are the respondent’s artificial intelligence techniques (including for example, the use of algorithms, ‘machine learning’ techniques, data mining techniques and automated decision making) audited, if at all?”* In their response, IPCO stated that they saw no examples of such artificial intelligence techniques and conducted no audits of such techniques.
11. I am able to address the extent of SIS’s capabilities and techniques in the area of “artificial intelligence” as it relates to SIS’s use of BPD. To do so, I have discussed this issue with colleagues in SIS who have particular expertise in this field.
12. I have seen the response from the MIS witness and confirm that I agree with their general statements on “artificial intelligence” as set out in paragraph 8 a-e.
13. I am unable to confirm or deny whether SIS carries out machine learning techniques when conducting BPD searches.
14. The Commissioners will be kept sighted on developments in this area. I can confirm that this area is subject to random audit by the Commissioners. Further details of Commissioner Oversight are detailed at paragraphs 19-21 (below).

*Search techniques*

15. During the course of the OPEN hearing, counsel for the Claimants based certain submissions on various assumptions about the way BPD is used by SIA, for example that it is used for the purposes of “profiling of entire populations and looking for behaviours” (transcript 1/88). In assessing the proportionality of SIS’s use of BPD, the Tribunal may

consider it helpful to understand further explanation of the nature of BPD searches, techniques typically employed by SIS staff searching BPD and the operational justification for using techniques in this way. In my amended statement of 8 July 2016, I set out the details of SIS's principal search tool, [REDACTED], and explained how safeguards are built in to the search tool (paragraphs 42-49), the proportionality of searching (paragraphs 20 and 22) and the mandatory training and guidance (paragraphs 50-57). [REDACTED]

16. BPD is accessed and exploited by the majority of analysts on the database for intelligence purposes. Within the database BPD analytical system, proportionality is inbuilt from the outset. Analysts are limited to specific fields when searching for data e.g. a telephone number. There is no "free text" capability. Analysts must have at least one piece of data (that they assess relates to an individual of interest) as a starting point, and SIS policy limits the analyst further as they are required to fill in as many fields as possible in order to minimise collateral intrusion. The fields are labelled to search against biographical data and selectors such as name, email address, telephone number. A necessity and proportionality justification must be recorded for searching against BPD.
17. Search results are ordered by relevance, and policy and training requires analyst to only review results which they assess to be associated with their intelligence requirement. Selection of chosen results (the database Summarisation) presents the analyst with further detail (e.g. the individual's travel) which cannot be reviewed in the initial search results and cannot be searched against. The analyst can view a sanitised description of the datasets to assist in assessing the relevance of the result.
18. At the date of writing, SIS hold [REDACTED] BPDs. The content and detail of the list of datasets are tightly held and the list has a high security classification to ensure its secrecy. This is both to protect the sources of the BPDs but also because it would not be necessary or proportionate for every member of SIS staff to have knowledge of all BPDs. The database analysts do not know when they commence a search what BPDs are available to be searched, which they are searching across or what they might hit on. The ability to deselect BPDs at the point of initial query in the database would be disproportionate and impede operational activity. In order to minimise the risk of intelligence failure, the initial search is conducted against all BPDs in the database by ensuring that possible matches against the initial search terms are not missed by restricting the query to specific data

sources. The analyst has the opportunity to restrict to specific data sources once the results have been reviewed.

[REDACTED]

*Oversight by Commissioners (including "random audit" or "dip testing")*

19. At pages 1/74, 1/85, 3/34 of the transcript, Counsel for the Claimants invited the Tribunal to conclude that the Commissioner has not carried out any random auditing of SIA BPD searches. I can confirm that this is not the case and reference was made to the auditing of searches at paragraph 59 of my previous amended statement dated 8 July 2016.
20. During each inspection, the Commissioner makes a selection of database "queries" to audit by selecting random dates and times from a calendar. On the last inspection visit 18 May 2017, four database searches were subject to specific scrutiny.
21. The Commissioner is provided with a report (extracted from the corporate record) detailing the date and time of the search, the details of the search (including search terms entered) and the designation of the analyst conducting the search. For example if the search was against the Name, Date of Birth and Nationality fields then the Commissioner will see these details in the report. The report also details the justification text entered by the analyst onto the database recording the necessity and proportionality for the search and a statement from the analyst explaining the operational context for the search. In addition to the report the Commissioner interviews the analyst to ensure that he is satisfied with the justification as described.
22. The Commissioner also carries out random audits in relation to other areas.
23. The Commissioner also audits the results of SIS's internal audit of the database searches which I referred to in my amended statement of 8 July at paragraph 61. He is provided with the audit investigation in the form of correspondence from the audit team to the individual concerned, the outcome/decision of the audit investigation (including any action taken) and any breaches that may have resulted.
24. At pages 87 to 88 of the transcript, I have seen that the Claimant's Counsel referred to the lack of technical understanding, within IS Com, of the SIAs' processing techniques. I refer to paragraphs 19-23 above and paragraphs 58 - 59 of my amended statement of 8 July 2016 in this regard. Further, and based on my own experience of dealing with the

Commissioners over a number of years, I believe that the Commissioner had a good understanding of how, in practice, SIS officers, including the [REDACTED], search our BPD holdings having attended two scrutiny visits per year since October 2010 which have included a number of demonstrations of the analytical tools.

*Action-on log*

25. During the course of their submissions at the OPEN hearing, counsel for the Claimants referred to the IPCO 2017 review of BPD (dated 15 September 2017). In paragraph 12 IPCO had questioned whether an action-on log specific to BPDs would be kept by an agency were sharing to take place, and counsel to the Claimants invited the Tribunal to infer that none existed. I cannot confirm in OPEN whether or not any sharing of BPD takes place. What I can say is that were any such sharing to take place, details of action on requests and resulting permissions or refusals would be recorded on the SIS corporate information management system rather than in any "action-on log". In such circumstances, requests, permissions or refusals would be available for the Commissioner to review. [REDACTED]

I believe that the facts in this witness statement are true

.....

Dated: