Witness: *GCHQ Witness*
Party: 3rd Respondent
Number: 8
Exhibit: *GCHQ13-14*
Date: 15.11.17

**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**

---

## WITNESS STATEMENT OF GCHQ WITNESS

---

I, **[Readacted]**, Deputy Director in the Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1. I am Deputy Director Mission Policy at GCHQ. This is my [Redacted] CLOSED witness statement in these proceedings. I have also prepared a number of OPEN statements.

2. I am authorised to make this witness statement on behalf of GCHQ. 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 the department.

3. 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, and that arose at the OPEN hearing on 15-17 October 2017. The particular issues are as follows:

   a) Clarification of points made in my seventh OPEN Witness Statement in relation to IOCCO s.94 audit.

   b) Provision of the paperwork that accompanied s.94 Directions when they were initially triggered.

   c) An update on the BPDs held by GCHQ and how we use them, including what techniques we use to analyse them.

   d) Details of GCHQ's holdings of social media data in BPDs.

   e) A description of GCHQ's use of Artificial Intelligence techniques with regards to BPD and BCD.

   f) Additional information regarding remote access to BPD and BCD.

   g) Additional information on the transfer of BPD and BCD.

   h) Correction and clarification of the situation regarding systems administrators.

**A. CLARIFICATION OF POINTS MADE IN SEVENTH OPEN WITNESS STATEMENT IN RELATION TO IOCCO s.94 AUDIT**

4. My seventh OPEN Witness Statement dated 18th October 2017 corrected a statement made at page 7 of the IOCCO report of their audit inspection of GCHQ conducted on 25-26 April 2017 under s.94 of the Telecommunications Act 1984. Paragraph 4 of my Witness Statement sets out the three elements which are captured and used for auditing purposes, namely (i) the authorised purpose for which they are conducting their search; (ii) an internal cross-reference which equates to a specific intelligence requirement; and (iii) a justification of the necessity and proportionality to access the data. Paragraph 5 of the Statement states that these three elements are made available to the Compliance Team, the IT Security Team and are provided to the IOCCO inspectors on demand.

5. Due to the wording of the recommendation in the IOCCO report, in the course of his submissions on 19 October 2017, the Claimant's Counsel interpreted this to mean that the IOCCO inspectors were only provided with the necessity and proportionality statement (element (iii) above) if they demanded to see it. This was

not the case. The IOCCO inspectors saw all three elements as outlined above, which included the necessity and proportionality statements. What "on demand" refers to here is the fact that the audit logs are additionally made available to IOCCO (and now IPCO) inspectors on any occasion outside of audit inspections, should they ask to see them. For the avoidance of doubt, the complete set of query data (statutory purpose, intelligence requirement, free-text justification) is included by default in the information provided to the inspectors when they conduct their annual audit review of the use of s.94 data.

6. There was a recommendation from the IOCCO inspectors that search terms should be included in the audit logs that they review and this change was implemented in June 2017 as described in paragraph 6 of my seventh Witness Statement.

**B. PAPERWORK ACCOMPANYING s.94 DIRECTIONS**

7. My fourth OPEN Witness Statement dated 16th June 2017 describes the process by which s.94 directions have been made and communicated to the CSPs to which they relate. Paragraph 9 explains that the provision of data under s.94 directions is triggered initially by a request from the Director of GCHQ. I attach as exhibit *GCHQ13* a selection of triggering letters for the assistance of the Tribunal. All of the triggering letters sent from Director to the CSPs were substantially identical to these.

8. It will be noted that there was a period of 7 weeks between the signing of Directions on 29 November 2001 and the sending of letters to the CSPs on 17th January 2002. The reason for the delay has not been documented but appears to be purely bureaucratic: records of internal emails show that 4 working days after the Direction was signed work was underway to draft and send the letters to the CSPs and it was acknowledged that this needed to be done swiftly. The note relating to the October 2016 Direction is undated but the metadata on GCHQ's EDRM system indicates that it was created no later than 17 October.

**C. UPDATE ON THE BPDS HELD BY GCHQ AND HOW WE USE THEM, INCLUDING WHAT TECHNIQUES WE USE TO ANALYSE THEM**

[Redacted]

9. Paragraphs 9-11 of my third OPEN Witness Statement dated 2nd March 2017 explains how we use BPDs and paragraphs 33-44 give some specific examples.

10. During the OPEN hearing the Claimant's Counsel suggested that BPDs are used for the "profiling of entire populations and looking into behaviours." Whilst BPD is held

about a large number of individuals, analysts will only actually look at the data relating to a small minority of those individuals. This is because of the way in which the BPD tools work: analysts ask specific questions of the data to retrieve information of intelligence value. For example, analysts might use travel-related BPDs to track the movement of targets, detect exploitable travel patterns of targets, identify new (previously unknown) targets, or infer activities/events of interest. [Redacted]. The purpose of this activity is to allow the analyst to establish the travel activities of a specific individual. It does not result in the creation of "profiles" of individuals not of intelligence interest.

**D. GCHQ'S HOLDINGS OF SOCIAL MEDIA DATA IN BPDs**

11. During the OPEN hearing, the Claimant's Counsel suggested that "social media" consisted of:

> *"not just Facebook; it is dating websites, apps and many other very sensitive sources. Such datasets, particularly if they're held in bulk, are highly intrusive, and they do contain information right at the very core of an individual's private life."*

[Redacted]

12. The ways in which a GCHQ analyst might use a social media BPD is to identify individuals who are of interest for a specific reason such as those using particular keywords, travelling to particular places, interacting with particular individuals or to gain behavioural insight into targets. Every query must be accompanied by a necessity and proportionality statement.

[Redacted]

**E. USE OF ARTIFICIAL INTELLIGENCE WITH REGARDS TO BPD AND BCD**

13. In the course of the OPEN hearing the Claimant suggested that the SIA make use of "artificial intelligence techniques" which, based on IPCO's response by email of 10 October to the Tribunal's letter of 2 October 2017, are not audited by the commissioners.

14. Paragraph 8 of the Security Service's [Redacted] Witness Statement dated 14 November 2017 gives a definition of the term artificial intelligence (AI) as it is used and understood by the SIA.

15. [Redacted] Two things should be noted regarding machine learning solutions (i) they can be very accurate, but only in proportion to the volume of truthed prior data, and this is typically expensive to generate (it often requires human input to have made judgments on the example data); (ii) because they entail approximation, they can yield false positives.

[Redacted]

**E. REMOTE ACCESS TO BPD AND BCD BY INTERNATIONAL PARTNERS.**

[Redacted]

**F. ADDITIONAL INFORMATION ON THE TRANSFER OF BPD AND BCD**

[Redacted]

## H. CORRECTION AND CLARIFICATION REGARDING SYSTEMS ADMINISTRATORS

16. In my seventh OPEN Witness Statement dated 18th October 2017 I explained in paragraph 10 that for some systems contractors may have administrator rights (known within GCHQ as a "Privileged User" (PU)). I explained that contractors only have privileged access during the design, build and testing phase and that once that was complete the administrator rights were passed to members of GCHQ staff. This is no longer the case. Following a change in policy introduced a few years ago there are contractors within GCHQ who are administrators of operational systems. This is because much of the hardware and software for these systems is provided by industry partners and they are therefore best placed to support those systems.

17. Privileged User accounts are divided into two categories, Privileged User Data and Privileged User Function. The policy governing the management of Privileged Users is exhibited as Exhibit *GCHQ14*.

18. PU Data access for staff who have been with GCHQ for less than 12 months and PU Function access where staff have been with GCHQ for less than 6 months is by exception and needs to be approved by the data owner.

19. Currently there are about 100 contractors with PU accounts for the main BPD and BCD repositories.

20. During the course of the OPEN hearing on 17 October 2017, the Claimants' Counsel submitted that there was nothing to stop "*a contractor with system access rights going to the system, getting the relevant data, and then covering their tracks*". The likelihood of that happening is low for the following reasons.

21. Command line interfaces (an interface which relies on the user typing commands into the computer, rather than interacting with a user-friendly interface using mouse and keyboard as one would do for example with Microsoft Windows software) are used by the PU community to manage the system (e.g. installing software patches, monitoring performance, investigating problems). There is system monitoring and auditing for malicious behaviours at the command line level. Additionally, the presentation of information using this interface is very basic. In order to do a simple search on the data you would need to consider the following:

    i. The data needs to be stored in a format which can be searched using a text string, or be converted into such a format

ii. Typically the data at rest on the data storage and retrieval platforms is not in a format which can be interpreted using the command line. The data is hosted in specialist file systems, databases or applications which hold the data in such a way as to optimise the data for the analysis being carried out using the appropriate managed interfaces.

iii. A simple example would be a Microsoft Word document which if accessed via the command line returns a garbled set of characters because the data needs to be placed through a Microsoft office converter to present the information into a readable textual format. The file would only be viewable as a proper document with the original layout and formatting if Word itself (or a compatible application) was used.

iv. The data needs to be stored in such a way to allow identification of a specific desired data item i.e. a data item may not be stored in one place, rather being distributed across a number of storage servers, which can only be reassembled using the specialist software.

22. The search tools available via the command line are basic and considering the scale of data which needs to be searched against they would time out (the search would fail due to exceeding the maximum time allowed by the system) or take an unreasonably long time to return any results.

23. Although the technical community would state in theory that it is at times possible to search for a string (e.g. a name) within the data using the command line, in practice this is not how the interface is used nor is the interface designed to enable this kind of use. Typically within GCHQ the level of complexity of the systems means the only way to access the data in a readable format is via the software APIs where necessity and proportionality auditing is implemented.

24. This is how system support is carried out within technical communities across the industry and it is considered reasonable behaviour. The additional training, screening and guidance we provide to those with PU access is there to enable compliance with the desired behaviours.

Statement of Truth

I believe that the facts stated in this witness statement are true.

GCHQ witness

.....

Dated: 15 November 2017