

Witness: GCHQ Witness
Party: 3rd Respondent
Number: 7
Exhibit: N/A
Date: 18.10.17

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 THE GCHQ WITNESS

I, the GCHQ Witness, 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. In that role, I am responsible for drawing up the operational policies that underpin GCHQ's intelligence gathering activities and for ensuring that they are complied with. I have been in this role since 5 January 2015, having previously served as Deputy to my predecessor. I have worked for GCHQ in a variety of roles since 1997.
- 2) I am authorised to make this witness statement on behalf of the Respondents. 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 further statement:
 - a) To clarify what is and has been made available to auditors when auditing searches of BCD made on GCHQ systems. In particular I wish to correct a statement made at page 7 of the IOCCO report of their inspection of GCHQ conducted on 25-26 April 2017 under s.94 of the Telecommunications Act 1984; and

- b) To address the references to system administrators made in IPCO's draft report of 15 September 2017.

(a) Information available to GCHQ auditors

- 4) As stated in the IOCCO report, analysts conducting searches must set out (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. It should be noted that this justification must be sufficiently detailed to allow another analyst, not directly involved in the operational activity, to determine whether it makes a sufficient necessity and proportionality case: this is the audit standard for this element of the search record.
- 5) All three of these elements are transferred to GCHQ's internal auditing system, together with details of the system or tool on which the query was run. In relation to what is stated at page 7 of the IOCCO report, at the dates of the inspection (25-26 April 2017), all of this information was (and continues to be) made available to both the Compliance Team and the IT Security Team for the purposes of their audit activity. The same data is made available to IOCCO inspectors on demand.
- 6) The specific search terms used in the query are also transferred to the auditing system. At the time of the IOCCO inspection these were not routinely presented to the auditors, but were retained and could be accessed if necessary. In June, in response to the IOCCO report, changes were made to the auditing system and the search terms are now returned for audit alongside the justification as a matter of course. For the avoidance of doubt, the nature of what would have been searched for would in any event have been apparent from the justification of necessity and proportionality of access to the data, and from the context of the particular systems or tools on which the query was run, even if the search terms themselves were not considered.
- 7) That explanation places what is said on page 7 of the IOCCO report in its proper context. I am not sure what was intended to be referred to by the statement that "*the two internal audits did not have access to the full detail of the FCHR justifications completed by the analyst*". However, the position is as set out above.
- 8) Page 7 of the IOCCO report also said that the internal audits did not have access to "*the data [the analyst] sought access to*". That statement was correct. The data returned by the query is not itself transferred to the audit system. This is because GCHQ does not consider it proportionate routinely to retain such data for such a long period.

(b) GCHQ system administrators

- 9) Paragraphs 14 and 15 of IPCO's draft report of 15 September 2017 refer to the possibility of "*a contractor with system access rights going into the system, extracting data and then covering their tracks*." It is important to set this statement in context.

10) It was explained to IPCO during their inspection that contractors may be involved in the design and build of systems that will hold BPD, and that for some systems contractors may have administrator rights. That is captured in the IPCO draft report. What is not captured, but which was also mentioned to the inspectors, is that once a system has been built it is transferred to a GCHQ staff systems administrator before any operational data is loaded. Contractor systems administrators will only have privileged access during design, build and testing on small amounts of test data. All contractors working on the development of operational systems are subject to the vetting and training requirements mentioned in paragraph 10 of my fifth witness statement. Contractors who act as systems administrators must also undergo additional, and more stringent, security checks as compared with other contractors. This is in order to provide GCHQ with a commensurately higher level of assurance before they are permitted to work as systems administrators.

Statement of Truth

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

.....

Dated:

