

Witness: GCHO Witness  
Party: 3<sup>rd</sup> Respondent  
Amended Number: 2  
Exhibit: GCHO 3  
Date: 06/03/17

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

---

AMENDED WITNESS STATEMENT OF GCHO WITNESS

---

I, GCHO 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 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) Documents referred to as exhibited to this statement are attached as Exhibit 'GCHO 3'.

- 4) Further to paragraph 95 of the Investigatory Powers Tribunal's judgment of 17 October 2016 and paragraph 4 of the Tribunal's order of 31 October 2016, I make this statement in order to:
- a) exhibit (for the convenience of the Tribunal) relevant sections of policies/handling arrangements relating to the sharing of BPD and BCD;
  - b) address the question as to whether GCHQ has, since avowal on 11 March 2015, shared bulk personal data ("BPD") (or a sub-set of BPD) with international partners and/or law enforcement agencies ("LEAs"), and if so, what restrictions as to transfer or use/retention were imposed by GCHQ; and
  - c) address the question as to whether GCHQ has, since avowal on 4 November 2015, shared s.94 bulk communications data ("BCD") (or a sub-set of BCD) with international partners and/or LEAs and if so, what restrictions as to transfer or use/retention were imposed by GCHQ.

**A. GCHQ'S POLICIES AND HANDLING ARRANGEMENTS RELATING TO THE SHARING OF BPD AND BCD**

- 5) I exhibit the following as exhibit GCHQ 3:
- a) Paragraph 16 of the Joint SIA BPD policy of Feb 2015;
  - b) Paragraph 5.2 (4<sup>th</sup> bullet), paragraphs 6.0-6.7 and paragraphs 8.1 of the cross-SIA BPD OPEN Handling Arrangements of November 2015;
  - c) Section 9 of the GCHQ CLOSED BPD Handling Arrangements;
  - d) Paragraphs 4.4.1 to 4.4.6 of the OPEN Handling Arrangements for BCD; and
  - e) Section 4.4 of the GCHQ CLOSED s94 Handling Arrangements.
  - f) Raw Data Release Request Form

**B. SHARING OF BPD/BCD WITH INTERNATIONAL PARTNERS AND LEAs**

- 6) Where members of foreign intelligence agencies are posted to GCHQ as liaison officers they are not given access to any of GCHQ's operational systems.
- 7) Were members of foreign intelligence agencies to be posted to GCHQ as integrated staff then they would be required to agree that they would comply with the same policies and safeguards that GCHQ employees are required to comply with. Were GCHQ to make any of its BPDs available to integrated staff from liaison partners and/or law enforcement agencies, or to grant access to systems containing BCD, GCHQ would require analysts to have completed all relevant training (including legalities training which would be required to be in date), to be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances. All queries would be accompanied by necessity and proportionality statements which would be audited by GCHQ. Analysts would be required to comply with GCHQ's Compliance Guide and other BPD/BCD policies and safeguards concerning access, retention and use. The treatment of LPP and journalistic material would be addressed in the required training, and as set out in the Compliance Guide. Such safeguards would put partner analysts on the same basis as GCHQ analysts.

- 8) Were GCHQ to grant access to any of its systems or databases containing BPD or BCD to international partners from their premises, it would be on the basis that all analysts given accounts on the system or database would have completed all relevant training, including in-date legalities training, and that they were assessed as having sufficient analysis skills together with all necessary nationality and security clearances. All queries would be required to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ. Analysts would be required to comply with GCHQ's Compliance Guide (which addresses *inter alia* the treatment of LPP and journalistic material) and all other extant BPD/BCD policies and safeguards concerning access, retention and use.
- 9) Whilst we can neither confirm nor deny whether the SIA have agreed to share or in fact do share BPD/BCD with either foreign liaison partners or LEA, were we to do so, we would
- Follow the principles and approach set out in our respective Handling Arrangements and policy/guidance.
  - Take into account the nature of the BPD and BCD that was due to be disclosed.
  - Take into account the nature/remmit of the body to which we were considering disclosing the BPD/BCD.
  - Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed.
  - Depending on the individual circumstance, seek assurances that the BPD/BCD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purposes of RIPA (in the interests of National Security, for the purpose of preventing or detecting Serious Crime, or for the purpose of safeguarding the economic well-being of the UK).
  - If relevant to the particular circumstance, seek assurances that its use was in accordance with the UK's international obligations.
  - Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the Agencies.
- 10) GCHQ operates on the basis that operational data of any sort may only be shared if it is necessary for one of GCHQ's statutory functions, and, as far as GCHQ's intelligence gathering function is concerned, in line with one of the three purposes for which that function can be exercised. This is set out in GCHQ's Compliance Guide. All sharing is subject to compliance with all relevant legal safeguards, and there is a requirement that recipients must accord the material a level of protection equivalent to GCHQ's own safeguards. The assessment of whether a partners safeguards meet this standard is a matter for the Mission Policy team, in partnership with departmental legal advisors and other specialist teams as appropriate. As a matter of policy GCHQ applies the safeguards required by RIPA to all operational data even if was not obtained under RIPA powers, so this is the standard that must be met. Sharing is also subject to policy approval by an appropriately senior member of the Mission Policy team, unless an explicit delegation of approval authority has been made. Policy approval may be subject to appropriate filtering or sanitisation of the data being applied to protect sensitive material or equities.

- 11) The Compliance Guide makes clear that, in line with the RIPA Interception of Communications Code of Practice, 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.

### C. SHARING OF BPD/BCD WITH INDUSTRY PARTNERS

- 12) 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 attached as Exhibit 'GCHQ 3'. It should be noted that this form is also used to seek approval for the sharing of certain non BPD/BCD data in specific circumstances.
- 13) GCHQ may share operational data (which might in principle include BPD/BCD) with industry partners for the purpose of developing and testing new systems. Actual operational data would only be shared for such purposes if it were not possible to use standardised corpuses of non-operational data. Any sharing would be of the minimum volume of data necessary to develop or test the system. In all cases the data would be the least intrusive data that can serve the purpose. For this reason any data known or believed to contain confidential information would not be used; similar data that does not contain such material would be used instead. Wherever possible data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that the data must be held on secure and accredited corporate premises in the UK.
- 14) All sharing of data with industry is recorded on a Raw Data Release Request form (exhibited at Exhibit GCHQ3) which must be completed by a member of GCHQ who is sponsoring the activities of the industry partner. This form (which is used for certain other forms of data sharing which do not involve BPD or BCD) requires the sponsor to describe the purpose of the sharing and the details of the data they wish to release. If the data is to leave GCHQ premises they must specify where it is to go, and how it will be transferred. The form requires the sponsor to detail the name, organisation and job title of the individual who will take responsibility for the data on receipt, how many people at the recipient organisation will have access, for how long the data will be retained and what will be done with it once the project is completed. These requests are assessed within the Mission Policy team and may be escalated up to the Deputy Director Mission

Policy where appropriate. Mission Policy will assess each proposal to ensure that the sharing is both necessary and proportionate, and may require modification of the request if there are concerns about proportionality.

Statement of Truth

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

GCRCQ Witness

Dated: 6 March 2017