Witness: GCHQ Witness
Party: 3rd Respondent
Number: 5
Exhibit: N/A
Date: Amended by witness on 7 July 2017, signed on 12 October 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 GCHQ WITNESS

I, 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 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 GCHQ.

3) On 15 June 2017 the Tribunal directed the Respondents to serve any OPEN, and if appropriate, CLOSED evidence in relation to BPD/BCD sharing with, and/or transfer to, industry partners by 4.30pm on Wednesday 21 June 2017. This statement is served in compliance with that direction.

4) This statement addresses the period from 2010 onwards.

5) There is a CLOSED annex to this statement that contains evidence relating to these matters that cannot be disclosed openly without causing damage to national security.

Existing evidence on GCHQ sharing of BPD/BCD with industry partners

6) At paragraphs 12-14 of my Amended Statement dated 6 March 2017, I provided the following information about GCHQ 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 'GCHQ3'. 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 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."

7) Further information about GCHQ's sharing of BPD/BCD with industry partners was set out in the Respondents' Re-Re-Amended Open Response to the Claimant's Request for Further Information dated 17 February 2017.

8) The purpose of this statement is to clarify and to expand upon this previous evidence concerning GCHQ sharing of BPD/BCD with industry partners.

Overview

9) GCHQ has contracts with a range of industry partners. These partnerships provide GCHQ with the technical capability that it needs to continue to deliver its mission at a time of rapid technological change. The approach GCHQ has adopted is to seek to use industry partners to deliver support services, allowing GCHQ to devote the efforts of its own technical staff to solving mission-based problems. In practice this means that industry partners deliver capabilities such as facilities and estates management, corporate services, data centre management, wide area networking and desktop provision, where GCHQ's requirements tend to mirror those of similarly-sized commercial organisations in the information sector. GCHQ also works with industry partners in the development of data storage and processing services, and the integration of commercially delivered services with other GCHQ-developed or commercially procured services, and the design, development, integration and support of operational systems, applications and infrastructure. GCHQ also lets contracts for research into emerging technologies, data science and similar fields of interest to the Department. GCHQ does not use contractors to conduct operational intelligence analysis.

10) These contracts cover the work of several thousand individuals. All those involved with operational systems are fully vetted. The great majority do their

work at GCHQ sites where they work under exactly the same conditions as GCHQ staff and use the same GCHQ infrastructure. They have the same training requirements for access to GCHQ systems as GCHQ staff in the same area and are subject to the same level of audit.

11) While, as noted above, GCHQ does not use contractors for operational intelligence analysis, it is necessary for some contractors to have access to operational data for the purposes of systems and applications development. This access may be on GCHQ operational systems, or through the provision of sample data for use within a new application while it is being developed. In all cases the data involved will be no more than is necessary for the purpose for which it is to be used.

12) The circumstances in which and the means by which industry partners access GCHQ data may be divided into three categories. First, industry partners access GCHQ data whilst using GCHQ equipment on GCHQ premises - i.e. in the same way that GCHQ staff access such data. Second, industry partners can be given remote access to GCHQ networks from their own premises. Third, data can be transferred to industry partners` premises for them to use at those premises. Each category is addressed below.

Definition of 'BPD'

13) There is a preliminary point that concerns the meaning of the term BPD in this litigation.

14) In a letter to GLD dated 15 June 2017, Bhatt Murphy cited the definition of a bulk person dataset that appears in the ISC (Additional Review Functions) (Bulk Personal Datasets) Direction 2015, which is as follows:

"any collection of data which ... comprises personal data as defined by section 1(1) of the Data Protection Act 1998 ... relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest [and] is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies"

Bhatt Murphy then asked for confirmation that *"a dataset of raw sigint data is a BPD within the meaning of the 2015 direction"*. A second question might be whether such a dataset is within the meaning of the term BPD as it has been understood throughout this litigation.

15) To address the first question, although a dataset of raw sigint data might as a matter of language meet the criteria of a BPD set out in the 2015 Direction, it is

clear from the context and purpose of the 2015 Direction that it was never intended to cover such datasets, and nor have such datasets ever been understood to be within its terms.

16) The 2015 Direction was issued following the avowal, through the publication of the Intelligence and Security Committee's March 2015 Report, that the Agencies acquired "*large databases containing personal information about a wide range of people*". The Committee distinguished Bulk Personal Datasets from intelligence obtained "*through capabilities such as interception*" (§151). They noted that oversight of Bulk Personal Datasets was the responsibility of the Intelligence Services Commissioner, but that it was conducted on a non-statutory basis. This is in contrast to the oversight of interception by the Interception of Communications Commissioner. They recommended that the Commissioner's role be put on a statutory footing. This was achieved through the 2015 Direction. It was not intended that raw intercept data would be subject to oversight by both the Interception of Communications Commissioner (further to his statutory role) and the Intelligence Services Commissioner (under the Direction).

17) There is (and was at the time of publication of the SIA BPD Handling Arrangements in November 2015) already an established regime for the handling of raw intercept data. Paragraph 10 of the SIA Handling Arrangements for BPD (which adopt the definition of BPD in the 2015 Direction) therefore reflects the intention that the Intelligence Service Commissioner's oversight should only extend to data that would not otherwise fall within the statutory remit of the Interception of Communications Commissioner.

18) The OPEN Handling Arrangements do however recognise the intention that where an Agency proposes to hold data derived from intercept (for example an attachment to an email) on its analytical systems (where it holds other BPDs) and the intention is to use that data for ongoing use/access by investigators, then that bulk dataset should be subject to the BPD Handling Arrangements. See, for example, paragraphs 2.8 and 2.9 of the SIA BPD Handling Arrangements (of November 2015).

19) This analysis is reinforced by the approach adopted in the Investigatory Powers Act 2016, where separate regimes govern, on the one hand bulk data acquired through interception, equipment interference, or communications data acquired by means of a bulk acquisition warrant (in Part 6), and on the other hand bulk personal datasets (in Part 7). See section 201(1) of the IPA 2016. As an exception to that default position, section 225 of the IPA 2016 expressly provides, consistently with the current approach (see previous paragraph), for a dataset

that has been acquired under a warrant (eg an interception warrant) to be retained and examined as BPD, if a direction to that effect is given by the Secretary of State (with approval of a Judicial Commissioner).

20) To address the second question, the Claimant's pleaded case uses the term BPD synonymously with the way in which that term was used in the March 2015 ISC Report, as discussed above. See in particular in this regard paragraphs 5-8 of the Re-Amended Statement of Grounds. I note also paragraph 9 of the Re-Amended Statement of Grounds, where the examples of BPDs given by Claimant do not include sets of sigint data (raw or otherwise). Accordingly, the Respondents have always understood that for the purposes of this litigation the term BPD has the same meaning as that ascribed to it by the ISC and the Intelligence Services Commissioner - i.e. that it excludes sets of raw data obtained under RIPA powers.

21) In summary, the Respondents do not accept that a dataset consisting of *"raw sigint data"* is either a BPD within the meaning of the 2015 Direction, or a BPD as that term has so far been used in this litigation.

Access to BPD/BCD by industry partners at GCHQ premises

22) A large number of contractors (several thousand), who are employed by industry partners, work on GCHQ premises using GCHQ IT equipment. This includes GCHQ premises outside of Cheltenham.

23) To summarise the position regarding contractors in this situation vis a vis access to BPD/BCD:

a) They only have access to data on GCHQ premises and on GCHQ equipment and GCHQ retains full control over the data they have access to.

b) They are subject to all the same vetting, training and justification requirements and auditing as GCHQ employees, some of which is outlined in paragraphs 60-66 of my witness statement dated July 2016.

c) Most of these contractors do not have any access to databases containing BPD or BCD.

d) Those that do (typically between 100-200 individuals) access BPD / BCD only when necessary for purposes of system maintenance and development.

24) To describe the position in more detail, any contractor needing to gain access to any database will have to apply for an account, putting forward a business case, and complete any relevant training before access is approved and granted. Use of the databases is monitored and searches of the data must be accompanied by a necessity and proportionality statement entered by the user. All industry partners and GCHQ employees are subject to the same governance arrangements in terms of mandatory training and compliance monitoring. Everyone must undertake Legalities training, the level of which is determined by the role they have been employed to do. Anyone with access to operational data must complete the relevant modules in the Advanced Mission Legalities training. For developers this would routinely include a module on Capability Development. Inline with GCHQ staff, those contractors who complete an Advanced Mission Legalities training module are also required to complete a monthly handling statement, the compliance of which is subject to internal monitoring.

25) For the avoidance of doubt, the paragraphs of my earlier statement that I have quoted above were not written with this type of `sharing` in mind. As will be apparent, the Raw Data Release Form is not relevant here. Moreover, although the necessity and proportionality requirements would prevent contractors accessing confidential data in almost all cases, there is no absolute bar on such access in this situation. It might be necessary for contractors to access sensitive data if, for example, maintenance or development work on a part of the system dedicated to holding material that included sensitive data required the running of test queries that resulted in the returning of such data.

Remote access to BPD/BCD by industry partners

26) Contractors employed by industry partners can be given access to GCHQ IT networks at their own (but GCHQ-accredited) premises. Only vetted individuals with a GCHQ IT account can access these terminals which have a reduced functionality compared to those located within GCHQ premises.

27) As with those contractors working within GCHQ premises, only a small number of individuals will have accounts that enable them to access databases containing BPD and BCD. They access these databases purely for the purposes of system development and maintenance.

28) All of the safeguards detailed at paragraph [24] apply equally to contractors working remotely, as do the comments that I have made at paragraph [25]

regarding the non-applicability of the Form and the ability in principle to access sensitive data..

29) GCHQ staff have undertaken checks of the records of databases being accessed remotely by contractors since 2010.

(a) There have been no instances of contractors accessing BCD remotely.

(b) One database containing BPD has been accessed remotely by a small number of individuals (fewer than 20) working for industry partners. All of these accesses were for the purposes of system testing and have occurred since 2015 when the database came into existence. We cannot demonstrate exactly what data was accessed on these occasions. However none of the BPDs held on this particular system were assessed as containing sensitive data, so it is highly unlikely that such data was accessed.

Transfer by GCHQ of BPD/BCD to industry partners

30) The process for the transfer of data to industry partners is described in the disclosed document [3/476], which was referred to in Bhatt Murphy's letter of 15 June 2017. This is an internal policy document that dates from 2011-15. The document has since been revised but the process remains the same. The document describes this process as "sharing sets of raw Sigint data". In fact the process and the form are used for sharing a range of operational data with partners, including, for instance, selected items of foreign language material believed to be of potential intelligence value which may be shared with e.g. SIS or MI5 for the purposes of translation. Data shared with industry under this process may be raw Sigint data, or data that has undergone some degree of processing and/or analysis, and is being shared with industry to enable the development of e.g. a data visualisation capability. For this reason I will use the term "operational data" which includes, but is not limited to raw Sigint data.

31) GCHQ shares samples of operational data with industry partners to enable them to develop systems and techniques that will improve GCHQ's capability to exploit the data. Samples of data are taken from GCHQ systems and transferred securely, often via removable media, to industry partners' own IT networks, which will have been accredited by GCHQ accreditors and will be accessed only within GCHQ-accredited premises or accredited areas within larger premises and by vetted staff.

32) The process for managing this transfer of operational data to industry partners is through completion of the Raw Data Release Request Form (Exhibit 'GCHQ 3') which must be submitted by a GCHQ sponsor and approved by the GCHQ policy team (up until about 2015 limited Delegated Release authority was also granted to specific individuals in the Research team for releases of data from their own area. We have no evidence that any approvals were made by this team). Further details of the form are given in paragraph 14 of the GCHQ Amended OPEN Witness Statement dated 6 March 2017, which I have quoted above.

33) GCHQ staff have reviewed all of the Raw Data Release Request Forms since 2010 and I understand that to the best of their knowledge there have been 51 transfers of operational data to industry partners during that time.

(a) No BPD has been transferred by GCHQ to industry partners in this period.

(b) As for BCD, in the period 2010-11 some samples of operational data that might have contained some section 94 data were transferred to an industry partners. The possibility that some BCD data was included in the operational data that was transferred arises from the relevant records, but it is not possible to be certain one way or the other because the samples have now been deleted. Specifics of how the samples were selected were not recorded (there is no indication that BCD sources were explicitly included or excluded and rather the approach appears to have been to get a large enough sample based on our accesses across a time period in order to be useful) so it is possible that it would have included data from our section 94 sources. One of the databases that the samples were extracted from (REDACTED) was a telephony events database and would have contained at least some s94 data. This database no longer exists so we cannot check what proportion of the entire dataset would have been derived from s94. As the samples have since been destroyed at our and the partner's locations we do not have any records of exactly what they included. The data was transferred via an encrypted laptop transported from Benhall to the partner's location via the secure courier service under a transfer mechanism approved by GCHQ accreditors. Except for the possible transfer in 2010-11, no BCD has been transferred by GCHQ to industry partners in this period.

(c) Further details are given in the CLOSED annex.

The University of Bristol

34) Paragraph 84(d) of the Claimant's recent skeleton argument reads as follows:
"One particularly important industry partner is the University of Bristol. Snowden documents indicate that researchers are given access to GCHQ's entire raw unselected datasets, including internet usage, telephone calls data, websites visited, file transfers made on the internet and others. Researchers are also given access to GCHQ's entire targeting database ("delivered ... at least once a day ..."), an exceptionally sensitive dataset."

35) The policy of Her Majesty`s Government is that it will neither confirm nor deny the authenticity of any of the documents published by *Wikileaks*. I am therefore not in a position to say anything about the documents to which the Claimant has referred. What I am able to do is to address the issue of substance, which is the nature of the relationship between GCHQ and the University of Bristol, and the extent to which that relationship involves the sharing of data.

36) GCHQ does have a partnership with the University of Bristol. The partnership is named the Heilbronn Institute for Mathematical Research and maintains a website at heilbronn.ac.uk. The partnership allows GCHQ to benefit from the expertise of academic researchers, in various mathematical and computational fields. The researchers split their time between GCHQ projects and other work.

37) The researchers` work for GCHQ is done in our premises in Bristol, and under the control of GCHQ staff who are stationed there. This work is done using GCHQ IT which is subject the same auditing and security controls as other GCHQ IT systems. The researchers are subject to the same vetting and mandatory training and legal safeguards as other staff. They are, in effect, contractors working at our premises. In other words, the `sharing` of data at Bristol falls into the first of the three categories detailed above.

38) The large majority of the researchers do not have any access to operational data. Their work focuses on solving mathematical problems and improving analytic techniques, so there is no need for them to access any operational data.

39) For those researchers who have access to GCHQ operational data, or have done so in the past, the data to which they have access is heavily circumscribed and restricted to what they need for their project. None of this data consists of BPD or BCD, nor has it in the past. These researchers' projects aim to improve our analytic tools and techniques using operational data, in a similar way to our use of industry partners.

40) We acknowledge that the University of Bristol is an important partner, and that our targeting database is an exceptionally sensitive dataset. The rest of paragraph 84(d) is untrue. Any operational data used by academics in the partnership at Bristol has been narrowly focused, has remained under our control, has been subject to full legal safeguards, and has been restricted to our IT systems.

Commissioner oversight of sharing

41) ~~The Commissioners~~ Sir Mark Waller and Sir John Goldring (respectively the outgoing and the incoming Intelligence Services Commissioner) and also Sir Adrian Fulford (the recently appointed Investigatory Powers Commissioner) have been briefed in general terms about GCHQ's use of industry in the course of their inspections of GCHQ. ~~The Intelligence Services Commissioner~~ Sir Mark Waller was specifically briefed in October 2015 and April 2016 on an aspect of this work when it resulted in the activities of industry partners being reflected explicitly in GCHQ's warrantry arrangements, although, as should be clear from the foregoing, the overwhelming majority of GCHQ's collaboration with industry partners does not involve activities requiring authorisation by warrants. GCHQ's work with industry partners was also raised with Sir Mark and Sir John at an inspection in October 2016 and with Sir Adrian in April 2017. Further information relating to these ~~is particular~~ briefings is contained in the CLOSED annex.

42) As far as BPD are concerned, industry access has been limited to access at GCHQ premises or remote access to data held in GCHQ repositories. The audit processes for these accesses are the same as the audit processes for access by GCHQ staff. There would therefore have been no additional oversight activity required as a result of the 2015 Direction over and above the Commissioner's oversight of GCHQ's use of BPD.

Statement of Truth

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

GCHQ witness

.....

Dated: 12 October 2017