

**B E T W E E N:**

**PRIVACY INTERNATIONAL**

**Claimant**

**-and-**

**(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS**

**(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT**

**(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS**

**(4) SECURITY SERVICE**

**(5) SECRET INTELLIGENCE SERVICE**

**Respondents**

-----  
**INDEX TO THIRD  
SUPPLEMENTAL BUNDLE**  
-----

1.	Order of the Tribunal	5 May 2017
2.	Letter Interception and Communications Commissioner's Office to Tribunal Secretary	27 April 2017
3.	Respondent's letter to the IPT	10 May 2017
4.	Respondent's re-amended Response to the RFI of March 2017	10 May 2017
5.	Respondent's outline response to Tribunal's questions of 8 March 2017	10 May 2017
6.	Amended OPEN version of GCHQ Policy for Staff from OGDs and SIA partners with access to GCHQ system data	
7.	Agreed text for IPT's letter to the Commissioners	12 May 2017
8.	UKUSA Agreement	5 March 1946

IN THE INVESTIGATORY POWERS TRIBUNAL  
BEFORE THE PRESIDENT AND  
SIR RICHARD MCLAUGHLIN

CASE NO. IPT/15/110/CH

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH  
AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

---

ORDER

---

UPON HEARING MR DE LA MARE QC AND MR JAFFEY QC FOR THE CLAIMANT AND MR EADIE QC, MR O'CONNOR QC AND MR O'BRIEN OF COUNSEL FOR THE RESPONDENTS AND MR GLASSON QC AS COUNSEL FOR THE TRIBUNAL AT A HEARING ON 5 MAY 2017

AND UPON HEARING SUBMISSIONS IN BOTH OPEN AND CLOSED SESSIONS

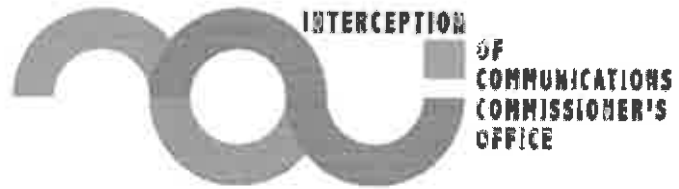
THE FOLLOWING DIRECTIONS ARE HEREBY GIVEN:

1. The Respondents to serve by 4pm Wednesday 10 May 2017:

- a. a revised outline response to
    - i. the questions identified by the Tribunal at the directions hearing on 8 March 2017; and
    - ii. the question as to whether the transfer of BPD (s) to the Security and Intelligence Agencies would amount to “data processing” as defined by Article 2(b) of the Data Protection Directive;
  - b. an amended OPEN and CLOSED response to the RFI dated 7 March 2017; and
  - c. its summary response to paragraph 14 of the Claimant’s Skeleton Argument dated 2 May 2017.
2. The parties are to liaise with Counsel to the Tribunal to use their best endeavours in order to agree by 4pm Thursday 11 May 2017 a draft letter for submission by the Tribunal to the Intelligence Services Commissioner and the Interception of Communications Commissioner (“the Commissioners”), further to the Commissioners’ letter to the Tribunal dated 27 April 2017.
  3. The parties are to use their best endeavours to serve updated bundles for the June hearing by 4pm on Monday 22 May 2017
  4. The parties are to inform the Tribunal immediately should it become possible to schedule an uninterrupted hearing in the week commencing Monday 5 June 2017. Otherwise, the hearing shall be listed to take place on Monday 5 June 2017, Tuesday 6 June 2017, Thursday 8 June 2017 (afternoon) and Friday 9 June 2017.
  5. The Respondents are to serve an amended OPEN Response and a CLOSED Response to the RFI on searches (dated 22 February 2017) by 4pm on Friday 30 June 2017.
  6. There shall be a hearing to determine the two issues identified in the Claimant’s Outline of Additional Issues dated 2 May 2017, such hearing to take place on Monday 31 July 2017 (time estimate one day). In relation to that hearing:

- a. The Respondents shall file and serve OPEN and CLOSED evidence pertaining to the two issues identified the Claimant's Outline of Additional Issues dated 2 May 2017 by 4pm on Friday 16 June 2017;
  - b. Counsel to the Tribunal to serve CLOSED submissions relating to such evidence by 4pm on Thursday 22 June 2017;
  - c. The Respondents to serve their response to Counsel to the Tribunal's submissions by 4pm on Thursday 29 June 2017;
  - d. The Counsel to the Tribunal and Counsel for the Respondents to meet before Wednesday 5 July 2017 to seek agreement if possible in relation to the issues raised by their respective submissions;
  - e. There shall be a CLOSED hearing on Friday 7 July 2017 to consider any issues arising from the disclosure submissions and any disclosure arising from that hearing shall be served by 4pm on Monday 10 July 2017;
  - f. The Claimant to serve its skeleton argument by 4pm on Monday 17 July 2017;
  - g. The parties are to use their best endeavours to serve updated bundles by Wednesday 19 July 2017;
  - h. The Respondents to serve their skeleton argument by 4pm on Friday 21 July 2017; and
  - i. If requested by the Tribunal, Counsel to the Tribunal shall file and serve a skeleton argument by 4pm on Friday 28 July 2017.
7. Liberty to apply.

**Dated 5 May 2017**



Susan Cobb  
Tribunal Secretary  
Investigatory Powers Tribunal

Thursday, 27 April 2017

Dear Sue,

**BULK COMMUNICATIONS DATA (BCD) AND BULK PERSONAL DATA (BPD)**

Thank you for your letter dated 13 April 2017, asking for the Interception of Communications and Intelligence Services Commissioners' assistance in relation to Privacy International v SSFCA and 4 others. I have set out answers below. Due to the short-frame of our reply we have limited our response to short factual replies, in so far as we have been able, to the Tribunal's questions.

**You asked 'In open the Tribunal invites the Commissioners to respond based on assumed facts whether, if a transfer of BCD and/or BPD to another agency or organisation, including a foreign agency, had taken place, they have regarded it as within their remit, and confirm that, in that event, they would have provided active oversight.'**

For BCD IOCCO has had oversight of s.94 directions since January 2015 (see para 2.1 of our review of s.94 directions published July 2016). The disclosures of bulk communications data (BCD) is within IOCCO's oversight and remit as set out in para 4.6.4 of the published handling arrangements for BCD (4.11.2015).

For BPD, section 10.2 of 'Arrangements under second 2(2)(a) of the Security Service Act 1989 and Sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 for obtaining and disclosing of bulk personal datasets, makes it clear that the use and disclosure of BPDs is overseen by the Intelligence Services Commissioner.

In both cases, use and disclosure is taken to include sharing with other agencies or organisations, including foreign agencies.

I hope this reply has been useful. Please do let me know if you have any further questions.

Yours sincerely,

Graham Webber  
Head of the Offices of the Interceptions of Communications and Intelligence Services  
Commissioners

## Section 2

# Background and purpose of the review of section 94 directions

### Background

2.1 The Prime Minister wrote to the former Commissioner in January 2015 to ask him to extend his oversight to include directions given by a Secretary of State under section 94 of the Telecommunications Act 1984. It was acknowledged that the Commissioner had previously provided *limited* non-statutory oversight of the use made of one particular set of directions by the Security Service. The Prime Minister was keen to extend that oversight.

2.2 The Commissioner responded that month agreeing to his role being extended and asked for clarification on the mechanism and authority under which the oversight would take effect. The Commissioner also highlighted a number of important points of detail that required careful consideration:-

- IOCCO had been working to improve the transparency of, and public confidence in, the oversight undertaken more generally. The Commissioner had expressed concerns to the Home Secretary previously about his inability to discuss publicly his *limited* oversight of one particular set of section 94 directions.
- For this reason the Commissioner's preference was for him to avow this oversight in his next half-yearly report (subsequently published in March 2015<sup>3</sup>).
- Clarification was required as to whether his function would include oversight of the necessity and proportionality of any section 94 directions; oversight of the use of the directions; oversight of the access to the material obtained pursuant to any direction (where relevant); and, oversight of the retention, storage and destruction arrangements for any material obtained (where relevant); and

---

<sup>3</sup> See Section 10 of March 2015 Report [http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20\(Web\).pdf](http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf)



# Government Legal Department

Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ

by email

Litigation Group  
One Kemble Street  
London  
WC2B 4TS

T 020 7210 3000

DX 123242 Kingsway 6

[www.gov.uk/gld](http://www.gov.uk/gld)

Your ref:

Our ref: Z1516543/EAO/N1

10 May 2017

Dear Sirs,

BPD IPT

We write by way of a response to paragraph 14 of the Claimant's skeleton argument dated 3 May 2017, as directed by the Tribunal at paragraph 1(c) of its order dated 5 May 2017.

The Respondents do not give the confirmation requested at paragraph 14 of the Claimant's skeleton argument. The position is as set out at paragraphs 4 to 10 of the M15 statement dated 10 April 2017, paragraphs 10 to 24 of the SIS statement dated 3 March 2017 and paragraphs 6 to 14 of the Amended GCHQ statement dated 6 March 2017, and at paragraph 7 of the Re-Amended Response of the Respondents to the Claimants' Request for Further Information and Disclosure dated 7 March 2017.

Yours faithfully,

Ellie Oakley  
For the Treasury Solicitor

D +44 (0)20 7210 8505

F +44 (0)20 7210 3152

E [ellie.oakley@governmentlegal.gov.uk](mailto:ellie.oakley@governmentlegal.gov.uk)

Sarah Goom - Head of Division  
Edward Holder - Deputy Director, Team Leader Litigation N1



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 COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

---

**RE-AMENDED OPEN RESPONSE OF THE RESPONDENTS  
TO THE CLAIMANTS' REQUEST FOR FURTHER INFORMATION  
AND DISCLOSURE DATED 7 MARCH 2017**

---

This document is the Response to the Claimant's Request for Further Information dated 7 March 2017 ("the RFI"). It is in two parts:

- Part 1: Response to Requests 1 to 6 of the RFI
- Part 2: Response to Requests 7 to 16 of the RFI

**PART 1**

**Of: the sample section 94 Directions**

- 1) Under Article 2(b) of Council Directive 95/46/EC ("the Data Protection Directive") the term "processing" is defined as meaning "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". Under Article 2 of the e-Privacy Directive the definitions supplied by the Data Protection Directive shall apply. In respect of each s.94 Direction that has been made (whether for internet, fixed-line telephone or mobile telephone BCD):
  - a) what activities amounting to processing within the meaning of the Data Protection Directive (set out above) are carried out by the PECN?



- b) To what extent does each PECN process data, extract it from other data, format it, or retain it pending transfer?
- c) Does any PECN retain data pending transfer? If so, for how long?
- d) Does any PECN use software or hardware to extract communications data from internet traffic or telephone calls, such as (but not limited to) by:
  - i) removing from an internet URL the path but not the hostname, pursuant to section 21(6) of RIPA 2000 (i.e. stripping out the communications data from the content provided after the 'first slash');
  - ii) carrying out deep packet inspection to obtain communications data; or
  - iii) any other means?
- e) Have payments been made to PECNs pursuant to s.94(6)? If so:
  - i) How much has been paid to PECNs over the last 5 years? When were payments made, and what were they for?
  - ii) Please disclose documents from and to PECNs seeking, negotiating and agreeing or refusing to make payments, and documentation supporting the payments made and the reasons for them.
- f) Please disclose documents recording the consultations with and any representations made by PECNs about s.94 BCD notices.

**Response to requests 1 (a), (b) & (c)**

**For the avoidance of doubt, the Respondents deny that the Data Protection Directive and/or e-Privacy Directive are engaged by the PECNs' provision of BCD to the SIA pursuant to s.94 directions. Subject to that qualification, the Respondents do not dispute that activities carried out by the PECNs pursuant to s.94 directions would amount to "data processing" as defined by Article 2(b) of the Data Protection Directive, were the Data Protection Directive and/or e-Privacy Directive to be engaged.**

**The precise nature of the processing that the PECNs carry out in order to fulfill their obligation to provide data to the SIA further to s.94 directions is not relevant. Without prejudice to that contention the Respondents make clear that in relation to each s.94 direction that is made in respect of any particular PECN:**

- (i) **the disclosure by transmission from the PECN to the SIA of BCD (and any minimal adaptation or alteration which may be necessary in order to separate or retrieve the data required to be disclosed from the PECN's**

wider data holdings which are not required to be disclosed, such as for example subscriber information) would amount to "data processing" by the PECN to that extent;

- (ii) the data provided to the SIA is held by the PECN, at the time of provision of it to the SIA, for the PECN's business use;
- (iii) in particular, the PECN does not hold that data (at the time of provision to the SIA) by virtue of (or as a result of) any obligation further to the s.94 direction;
- (iv) the s.94 direction does not require the retention of data by the PECN; and
- (v) for the avoidance of doubt, neither do the SIA request the PECN to retain any data for the purposes of their providing that data to the SIA further to the s.94 direction.

**Response to request 1 (d)**

The Respondents are unable to answer this request in OPEN. A CLOSED response has been served. In any event, in light of the Respondent's concession regarding processing, this request is now irrelevant to the issues in dispute.

**Response to request 1(e)**

Whether or not payments have been made (or the amount of any payments) is not relevant to the issues in this claim.

**Response to request 1(f)**

The relevance of such documents is denied.

- 2) Please disclose any guidance, requirements or information provided to PECNs specifying the processing, formatting or other arrangements affecting BCD that apply to them.

**Response to request 2**

There is no guidance, requirements or information provided to PECNs specifying the processing, formatting or other arrangements affecting BCD that apply to them.

The only additional processing carried out by the PECN (beyond the disclosure of the BCD by transmission from the PECN to the SIA) is such minimal adaptation or

alteration as may be necessary in order to separate or retrieve the data required to be disclosed by the s.94 direction from the PECN's wider data holdings which are not required to be disclosed.

- 3) Please provide full particulars of the precise nature and extent of the delegation of powers or authority to select what communications data is provided, when, in what circumstances and to whom and how such delegation has been exercised by:
  - a) the Director of GCHQ;
  - b) any person authorized by him to make such request (including the civil service level or grade of such person);
  - c) the Security Service (including the civil service level or grade of such person); and
  - d) any other person (whether a public official or otherwise)?
- 4) On what basis is the Secretary of State satisfied that the GCHQ section 94 Direction is in accordance with the law and proportionate in circumstances where the data to be collected are:
  - a) not identified (*"will include but are not limited to"*); and
  - b) may be altered by the Director of GCHQ without the prior approval of the Secretary of State?
- 5) What procedures and arrangements are in place when the Director of GCHQ or any other person alters the requirements for data sought pursuant to a section 94 Direction?

#### Response to requests 3-5

The form of section 94 direction used by the Home Office, a (redacted) sample of which has been disclosed, does not confer any subsidiary or consequential powers on the Security Service or anyone else. It is simply an order made by the Home Secretary requiring the named PECN to provide specified communications data to the Security Service.

The form of section 94 direction used by the Foreign Office, a (redacted) sample of which has also been disclosed, also identifies specified communications data that (in this case) the Foreign Secretary determines is necessary to be provided (in this case) to GCHQ in the interests of national security. Paragraph 2 of the direction creates a power in the Director of GCHQ (or a person nominated by him) to trigger the operation of the direction by making a formal request to the named PECN. In the case of every section 94 direction made by the Foreign Secretary, a request under paragraph 2 has always been made immediately following the making of the direction. It is denied that either paragraph 2 or any other provision of the direction creates a power on the part of the Director of GCHQ or any other official either to select (i.e. to reduce) or to alter the specified communications data that the named PECN is required to provide under the express terms of the direction

signed by the Foreign Secretary. For the avoidance of doubt, neither the Director of GCHQ nor any other official has ever sought to exercise such a power.

The stipulation in the FCO section 94 notice that the data to be provided include *"but are not limited"* to the data set out on the notice is intended to serve a similar function to section 5(6) of RIPA, that is to enable the PECN to supply data beyond that described on the notice if that is necessary in order to supply the data that is described on the notice.

- 6) Please disclose any submissions or representations made to the Secretary of State in support of the section 94 Directions disclosed.

**Response to request 6**

These documents have already been disclosed to the Tribunal on a voluntary basis in CLOSED. For the avoidance of doubt, it is not accepted that these documents are relevant to the current proceedings.

## PART 2

- 1) This is a response to requests 7 to 16 of the RFI. The context of the RFI is a situation in which the Respondents have already served OPEN and CLOSED evidence and OPEN and CLOSED responses to an earlier Request for Further Information (dated 17 February 2017) covering the same ground, together with a lengthy Annex to the Respondents' skeleton argument of 3 March 2017. The Claimant complains that the earlier requests have not been answered. The Respondents' position is that the requests have been fully answered in CLOSED (whether in evidence or by way of response to the earlier Request for Further Information), and that OPEN disclosure of that material has been made where possible. This document contains some further information, but for the avoidance of doubt this document is intended to supplement rather than to replace the earlier documents mentioned above.
- 2) The Claimant has raised on more than one occasion the non-disclosure of written policies and related documents. However, the Respondents have disclosed such policies and documents: see the Annex to the skeleton dated 3 March 2017, including the references in that Annex to the Respondents' policy documents. Further, the Respondents have served some documents in CLOSED which have been gisted in OPEN evidence. In addition, there are established practices which are not the subject of written policies but which the Respondents have described in evidence/responses to RFIs/the Annex to the 3 March skeleton (including some such that are described in OPEN for the first time here). If and insofar as any legal implications arise from the fact that these established practices were not previously written down and/or published, they have in fact now been written down and published in the aforementioned documents.

### Commissioners

- 3) The Intelligence Services Commissioner and Interception of Communications Commissioner have oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD compliance (as applicable), including that relating to any form of sharing or provision of remote access, were it to occur. The Tribunal has upheld the adequacy of the Commissioners' oversight throughout (at least) the post-avowal period.<sup>1</sup> See also:
  - a) BPD: The Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015, pursuant to which the Prime Minister, pursuant to his power under s.59(a) of RIPA, directed the Intelligence Services Commissioner to "*continue to keep under review the*

---

<sup>1</sup> Since 2010 in the case of BPD and since July 2015 in the case of BCD (October 2016 judgment, §§80-82).

*acquisition, use, retention and disclosure by the [SIAs] of bulk personal datasets, as well as the adequacy of safeguards against misuse.” and to “assure himself that the acquisition, use, retention and disclosure of bulk personal datasets does not occur except in accordance with” the relevant sections of the SSA 1989 and ISA 1994 and to “seek to assure himself of the adequacy of the [SIAs’] handling arrangements and their compliance therewith.” (emphasis added) (see Annex to Respondents’ skeleton of 3 March 2017, §33).*

- b) BCD: the Interception of Communications Commissioner has oversight over all aspects of disclosure of BCD: See Annex, §66 and:
  - i) MI5 BCD Handling Arrangements of November 2015, §4.6.4(b): *“The Interception of Communications Commissioner has oversight of...(b) MI5’s arrangements in respect of acquisition, storage, access...and subsequent use, disclosure, retention and destruction”* (emphasis added); and
  - ii) GCHQ BCD Handling Arrangements of November 2015, §4.6.9: *“The Interception of Communications Commissioner is responsible for overseeing [inter alia] disclosure...of the data”*.

#### Action On

- 4) The Respondents have previously referred to “Action On” in the context of sharing of BPD and BCD. This has prompted a number of requests for further information from the Claimant. The Respondents wish to put the “Action On” mechanism in its proper context, and also make clear that, whilst this mechanism is regarded as a crucial safeguard, it cannot be regarded as a complete safeguard in the field of BPDs and BCDs.
- 5) “Action On” is a mechanism for ensuring that the Security and Intelligence Agencies retain control over information that they have disclosed to partners. It would apply equally to the sharing of BPD/BCD as to other intelligence sharing. In general terms, the mechanism would prevent information contained in a BPD or BCD that was disclosed to a partner being acted on or being passed to a third party without the originating service’s consent. To that extent, the Respondents rely on it as a safeguard in the sharing context. Precisely what proposed action would trigger the ‘action on’ mechanism in any given case would depend to an extent on the partner in question and the nature of the BPD/BCD involved. It would be likely to apply to disclosing the BPD/BCD, a sub-set of a BPD/BCD or an individual piece of data from a BPD/BCD to a third party, and to taking executive action based on it, for example detaining an individual on the basis of information from a BPD/BCD. For the avoidance of doubt, however, the Respondents do not contend that the mechanism would be triggered by holding, accessing or searching BPD/BCD, by preparing intelligence reports on the basis of BPD/BCD or by disclosing such intelligence reports back to SIA.

Security Service policy on sharing BPD/BCD

- 6) Some detail as to the policy that the Security Service would adopt were it to share BPD/BCD is set out in the Annex §§28-30, 42-46, 64, 74-76. Further detail as to the Security Service's policy in this regard is as follows:
- a) The overall scheme of the principles of sharing would be:
    - i) An information gathering exercise would be conducted in relation to the proposed recipient.
    - ii) If that was satisfactory, then a sharing agreement would be prepared, if deemed necessary, to reflect the matters that the Security Service considered (having regard to the information gathering exercise) needed to be covered.
    - iii) Individual consideration of each bulk dataset to be shared would be carried out. If agreed, then any sharing of bulk datasets would be accompanied by specific handling instructions, setting out any particular requirements considered appropriate.
    - iv) Ongoing review of the sharing relationship would be conducted.
  - b) Stage 1 – information gathering: In advance of initial sharing, and to inform the decision-making process to do so, an information gathering exercise would be undertaken to better understand the legal framework, policy and practice of the recipient. Specifically this exercise would gather information in the following areas which would inform decision making and any written agreements that were deemed appropriate:
    - i) Law and Policy – identifying the legal and policy regime that would apply in relation to bulk datasets in the recipient.
    - ii) Acquisition of Bulk Data – identifying (if any) the process which would be applied before the recipient acquires bulk datasets and whether there is any legal and/or policy obligation to consider the necessity and proportionality of acquiring a particular dataset.
    - iii) Authorisation – identifying the process and requirements (if any) that would be applied to authorise the retention and examination of bulk datasets.

- iv) Ingestion and Access – identifying how shared data would be stored, any categories of data they consider sensitive (for example LPP) either by law or policy and any policy governing access to the raw dataset or intelligence derived from it.
  - v) Exploitation and Analysis – make reasonable enquiries regarding the use that would be made of the bulk data and the capabilities of the systems on which it would be used.
  - vi) Disclosure – identifying any ACTION ON procedures or safeguards and the considerations taken into account when deciding to share bulk data with others.
  - vii) Retention and Review – identifying the process and parameters by which the necessity and proportionality case for continuing to retain and exploit bulk data would be reviewed.
  - viii) Oversight – identifying what internal and external oversight arrangements would be in place to audit the acquisition, retention and exploitation of bulk data.
- c) In addition, in the event of any sharing of bulk data outside the SIA, the Security Service would ensure that sharing of that data is in accordance with any wider HMG policies which the Security Service is required to adhere to (for example HMG Consolidated Guidance).
- d) Stage 2 – Sharing agreement: Subject to the Security Service being satisfied following its information gathering exercise, a written agreement would, if considered necessary, be agreed between the recipient and the Security Service in advance of any bulk data sharing. Insofar as considered appropriate, the Security Service would require the recipient to apply safeguards to the handling of any shared bulk data which corresponds to the Security Service’s domestic requirements.
- e) Stage 3 – Individual consideration of each bulk dataset to be shared and the terms of handling instructions to accompany each bulk dataset shared.
- i) In every instance where sharing of bulk data were proposed then there would need to be particular consideration of that proposed sharing, having regard to the terms of any sharing agreement in place.
  - ii) In each case where a bulk dataset were shared with a partner, specific handling instructions would accompany it.



- iii) In addition, insofar as considered appropriate, the Security Service would require the recipient to apply specific safeguards to the handling of any shared bulk data which correspond to the Security Service's domestic requirements appropriate to the nature of the data being shared.
- f) Stage 4 - Review: were sharing of bulk data to occur, the Security Service would maintain the following ongoing obligations:
  - i) Undertake reviews to ensure the necessity and proportionality case for sharing continued to exist.
  - ii) Undertake reviews of the adequacy of the arrangements governing the sharing with each recipient, including Action On, as and when necessary.
  - iii) End current sharing with a recipient if judged necessary as a result of the above.
  - iv) Inform the recipient of any changes to the Security Service's legal obligations impacting on bulk data sharing and update, as necessary, any written agreements and/or handling instructions.

#### Equivalent standards

- 7) The Claimant has requested further information as to whether the SIAs would require partners to comply with "*equivalent standards*" to those set out in their own handling arrangements. The position of the SIAs is that, were sharing to take place, insofar as considered appropriate they would seek to ensure that the recipients afforded the information an equivalent level of protection to the SIAs' own safeguards. This would be effected in appropriate cases by the procedures set out above and in the Respondents' witness statements, including requiring the proposed recipient to apply safeguards to the handling of any shared bulk data which corresponded to the SIAs' own domestic requirements.

#### Individual requests

Of the GCHQ witness statement of 6 March 2017

7. Are the matters at paragraphs 7 and 8 of the witness statement recorded in a written policy? If so, what is the date of the policy? Please disclose it.

**As to request 7:**

- a) **As to the matters set out in paragraph 7 of GCHQ's witness statement, an OPEN version of a policy document dated July 2013 that makes provision for integreees at GCHQ from UK OGDs and SIA partners is attached.**

- b) The matters set out in paragraph 8 of GCHQ's witness statement are not recorded in a written policy.

8. Do the matters in paragraphs 7 and 8 apply to granting any remote access to law enforcement agencies and/or international partners who are not integrated staff or on GCHQ's premises?

As to request 8, the terms of paragraphs 6 to 8 of GCHQ's witness statement of 6 March 2017 are clear in respect of international partners. They would also apply to Law Enforcement Agencies, were remote access to be granted to them.

9. Do the matters in paragraphs 7 and 8 apply to sharing with industry partners? In particular, are staff of industry partners required to:

- a) comply with the same policies and safeguards as GCHQ staff;
- b) complete all relevant training, including legalities training;
- c) be assessed as having sufficient analysis skills;
- d) have security clearance;
- e) accompany all queries by necessity and proportionality statements;
- f) have such statements audited by GCHQ;
- g) comply with GCHQ's compliance guide; and
- h) comply with the same safeguards in relation to the treatment of LPP and journalistic material as GCHQ staff?

As to request 9, the answer to each of the individual sub-paragraphs is "Yes", save that:

- a) In relation to request 9(c), staff of industry partners are not required to have "*sufficient analysis skills*". Bulk data is not provided to industry partners for the purpose of analysis but for the development of GCHQ's systems;
- b) In relation to requests 9(e) and (f), where bulk data remained within GCHQ's own IT infrastructure all queries would be required to be accompanied by necessity and proportionality statements and would be auditable, but not otherwise;
- c) In relation to request 9(h), industry partners are never provided with data known or believed to contain confidential information. The safeguards in relation to the treatment of LPP and journalistic material, although in theory applicable, are therefore very likely to be irrelevant in practice.

Of the MI5 witness statement

10. GCHQ requires that "recipients must accord the material a level of protection equivalent to GCHQ's own safeguards". Does MI5 apply the same requirement, *mutatis mutandis* to any:

- a) sharing with UK Law Enforcement Agencies;
- b) sharing with industry partners; and
- c) sharing with foreign liaison partners?

Please disclose the relevant arrangements evidencing the answers.

**As to request 10, see "Security Service policy on sharing BPD/BCD" above.**

11. In particular, does MI5 require that any UK Law Enforcement Agency, industry partner or foreign liaison partner each:

- a) comply with the same policies and safeguards as MI5's staff;
- b) complete all relevant training, including legalities training;
- c) be assessed as having sufficient analysis skills;
- d) have security clearance;
- e) accompany all queries by necessity and proportionality statements;
- f) have such statements audited by MI5;
- g) comply with MI5's arrangements; and
- h) comply with the same safeguards in relation to the treatment of LPP and journalistic material as MI5 staff?

**As to request 11, see "Security Service policy on sharing BPD/BCD" above.**

Of the SIS witness statement

12. Of paragraph 12, is "equivalent standards" a requirement of SIS's policy and arrangements, or an objective which is aimed for but may not always be achieved before sharing may be permitted?

**As to request 12, see "Equivalent standards" above.**

13. GCHQ requires that "recipients must accord the material a level of protection equivalent to GCHQ's own safeguards". Does SIS apply the same requirement, *mutatis mutandis* to any:

- a) sharing with UK Law Enforcement Agencies;
- b) sharing with industry partners; and
- c) sharing with foreign liaison partners?

Please disclose the relevant arrangements evidencing the answers.

**As to request 13, see "Equivalent standards" above.**

14. In particular, does SIS require that any UK Law Enforcement Agency, industry partner or foreign liaison partner each:

- a) comply with the same policies and safeguards as SIS's staff;
- b) complete all relevant training, including legalities training;
- c) be assessed as having sufficient analysis skills;
- d) have security clearance;
- e) accompany all queries by necessity and proportionality statements;
- f) have such statements audited by SIS;
- g) comply with SIS's arrangements; and
- h) comply with the same safeguards in relation to the treatment of LPP and journalistic material as SIS staff?

The matters requested in request 14 have already been addressed in SIS's witness statement dated 3 March 2017, save that SIS also confirm that they would apply to sharing with industry partners, were it to occur.

Of paragraph 21, would each of the following constitute "Action-On"?

- a) holding BPD;
- b) aggregating BPD with a foreign liaison service's own datasets;
- c) searching BPD;
- d) searching BPD for legally privileged or journalistic material;
- e) preparing intelligence analysis on the basis of BPD searches;
- f) disclosing such an intelligence report to SIS;
- g) disclosing such an intelligence report outside of foreign liaison service to a foreign Minister responsible for the liaison service or equivalent;
- h) disclosing such an intelligence report to an intelligence agency in a third country; and
- i) detaining a person based on such a report?

**As to request 15, see "Action On" above.**

16. The Claimant renews its requests for disclosure of the unanswered requests in the RFI dated 17 February 2017

**As to request 16, the Claimant has confirmed (by letter dated 9 March 2017) that requests 1-3, 4b-e, 5-17, 20 and 22 of the 17 February 2017 RFI are renewed, and specifically asserts that *"although certain of the question have been answered in part...the relevant policies have not been disclosed; and no information has been provided as to the extent or otherwise of the audit and oversight in fact carried out by the Commissioners"*. As to that:**

- a) **All relevant policies have now been disclosed; and**
- b) **The Respondents has already responded in relation to the Commissioners in its Response to the 17 February 2017 RFI and the Annex to the skeleton argument dated 3 March 2017 (see above). The Tribunal has already considered, and upheld, the adequacy of Commissioner oversight. Nothing further requires to be disclosed.**

**28 MARCH 2017**

2 MAY 2017

10 MAY 2017

**ANDREW O'CONNOR QC  
ROBERT PALMER  
RICHARD O'BRIEN**

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
- (2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
- (3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
- (4) SECURITY SERVICE
- (5) SECRET INTELLIGENCE SERVICE

Respondents

---

RESPONDENTS' OUTLINE RESPONSE  
TO THE TRIBUNAL'S QUESTIONS OF 8 MARCH 2017

---

1. This is the Respondents' more developed outline response to the Tribunal's three questions of 8 March 2017, filed pursuant to the direction of the Tribunal at the hearing on 5 May 2017. The Respondents will further develop their response in their skeleton. The Respondents also provide further clarification of their position on whether "processing" within the meaning of Article 2(b) of the DPD happens upon the accessing of BCD and/or BPDs, as requested by Counsel to the Tribunal.

***Q1 & Q2: Did the CJEU in deciding the issues it did in Watson, in relation to retention of and/or access to databases for the purposes of national security, have jurisdiction in the light of Article 4 TEU? In the light of Article 4 TEU, what is the effect of its judgment in Watson on the Tribunal's decision in this case?***

2. The Respondents' primary position is that the CJEU confined its judgment in *Watson* to the issues concerning the retention of and/or access to data for the purposes of the investigation, detection and prosecution of serious crime. It made no findings in relation to the retention of and/or access to data for the purposes of national security.

Such matters fall outside the scope of EU law (see Art 4(2) TEU). The question of jurisdiction is thus not engaged because the CJEU did not make findings that would have engaged that issue.

3. *Tele2/Watson* was not concerned with the legal regimes governing the UK Intelligence Agencies' acquisition and use of BPD or BCD. The CJEU was concerned with the application of the E-Privacy Directive ('EPD') to Member States' communications data retention schemes in the context of criminal investigations. Those schemes replaced EU-wide arrangements and are (at least in part) within the scope of EU law. By contrast, the legal frameworks governing the SIAs' acquisition and use of BPD and BCD, which are to be found in the Intelligence Services Act 1994, the Security Service Act 1989 ('ISA/SSA') and in section 94 of the Telecommunications Act 1984, do not implement EU law and the EU Charter therefore does not apply. It is clear from the Treaties that National Security remains the sole responsibility of the Member States in accordance with Article 4(2) TEU. Further, in the context of BPD, the CJEU did not purport to consider the Data Protection Directive.
4. Alternatively, if and to the extent that the CJEU's judgment might suggest that it purported to make any findings in relation to the retention of and/or access to databases for the purposes of national security, it had no jurisdiction to do so in light of Article 4 TEU. In particular, by virtue of Article 4 TEU, the CJEU had no jurisdiction to review the actions of the intelligence agencies in acquiring and accessing such databases. On this alternative basis, the CJEU would appear to have reached a decision which overstepped the jurisdictional limits that the Member States had clearly set at the European Treaty level.
5. In those circumstances, the judgment must be read, and can be read, so as to avoid the conclusion that the CJEU assumed a jurisdiction it did not have. In particular, it is to be noted that the judgment in *Tele2/Watson* did not consider Article 4 TEU and its effects; and did not seek to address the issues as to jurisdiction that that Article entails. As such, any ambiguity as to scope of the judgment can be resolved by reading the judgment consistently with the scope of the jurisdiction conferred on the EU, and therefore on the CJEU, by the Treaties.

6. There is a further alternative argument. Pursuant to this further alternative argument the Tribunal would be under no obligation to treat itself as bound by the CJEU's judgment (insofar as the judgment is incapable of being read consistently with the jurisdictional limits that Member States have set at the European Treaty level and which are reflected domestically in national law, i.e. insofar as the judgment could only be read as relating to the activities of UK intelligence agencies, or the use of data acquired by them). The argument would be that the Tribunal (as the relevant domestic court) has sole jurisdiction to review the legality of such activities as a matter of domestic law and Parliament has not conferred on the CJEU unlimited as well as unappealable power to determine and expand the scope of EU law irrespective of what the Member States clearly agreed in the Treaties. The basis of such an argument is set out in *Pham v Secretary of State for the Home Department* [2015] 1 WLR 1591 at §90, *per* Lord Mance (with whom Lord Neuberger, Lady Hale and Lord Wilson agreed). This argument, flagged in the Supreme Court as indicated, is a controversial one given the potential for conflict between UK law and EU law as interpreted by the CJEU. The Respondents do not yet have a final, cleared position on whether to advance this argument; and so cannot and do not positively advance it at this stage. Such a position is being sought urgently and the Tribunal will be informed of the final position as soon as possible.
7. The Respondents' position in any event will be that it is not necessary for the Tribunal to go this far. In accordance with the Respondents' primary and alternative submissions set out above, the CJEU did not, and did not purport to, address matters outside its competence; and to the extent there is any ambiguity, the judgment should be read consistently with the scope of EU law as conferred by the Treaties.

***Q3: What is the effect, if any, on issues 1 and/or 2 and/or on the CJEU's jurisdiction of the fact that BCD and/or BPDs may be used for the prevention or detection of crime?***

8. As explained in the Respondents' skeleton argument at §3.3 and §§26-35, the use by law enforcement agencies of BCD and/or BPDs acquired by the intelligence agencies falls outside the scope of the DPD and e-Privacy Directive: the use of BCD and/or BPDs for the prevention or detection of crime falls within the "*activities of the State*" referred to in Article 3(2) of the DPD and Article 1(3) of the e-Privacy Directive. The

CJEU's judgment in *Watson* is premised upon the application of those Directives and does not apply to the use of such data.

***Q4: Clarification on "processing" within the meaning of Article 2(b) of the DPD***

9. Counsel to the Tribunal requested the Respondents to respond to the following additional question arising from their response to the Claimant's RFI requests 1 and 2: "Does the response that the Respondents have given amount to a concession that there is processing which would engage the Directives if they apply and hence render it impossible to distinguish *Watson* if it applies"?
10. In their response, the Respondents made clear that it is denied that the Data Protection Directive and/or e-Privacy Directive are engaged by the PECNs' provision of BCD to the Security and Intelligence Agencies pursuant to s.94 directions. Subject to that qualification, the Respondents did not dispute that activities carried out by the CSPs pursuant to s.94 directions would amount to "data processing" as defined by Article 2(b) of the Data Protection Directive, were the Data Protection Directive and/or e-Privacy Directive to be engaged.
11. Alternatively, if the Directives were to be engaged (contrary to the Respondents' case), *Watson* should still be distinguished. A different proportionality balance may be struck, having regard to the importance of the purpose for which the data is processed (that is, the purpose of national security), and the wide margin of discretion that the Member States enjoy in judging the necessity for such processing in the interests of national security. For the reasons identified from §58 et seq. of the Respondents' skeleton argument of 2 March 2017, the safeguards identified in *Watson* are neither necessary nor appropriate to ensure the proportionality of Intelligence Agencies' access to BCD and BPDs.
12. For the avoidance of doubt:
  - 12.1. The proportionality balance does not depend on any evidence as to the extent of the "processing" that takes place in order to transfer the BCD to the Respondents. As set out in the Respondents' Response dated 28 March 2017 to the Claimant's Request for Further Information, any adaptation or alteration as may be necessary



to separate or retrieve the data is minimal in nature. Nothing turns on any detail of the precise details of the processing undertaken.

12.2. If, contrary to the Respondents' primary case, the Data Protection Directive applies to the acquisition by the SIAs of BPDs from third party providers of BPD, it is accepted that this may also involve "processing" by those third parties within the meaning of the Data Protection Directive, assuming that the processing activities of those third parties fall within the scope of the Data Protection Directive.

**JAMES EADIE Q.C.**

**GERRY FACENNA Q.C.**

**ROBERT PALMER**

**10 May 2017**

# **GCHQ Policy for Staff from OGDs and SIA partners with access to GCHQ systems and data (Part I)**

## **I. Introduction**

1. Staff on loan to GCHQ from other government departments (OGD), including the UK's intelligence and security agencies and other UK customer organisations, are a welcome and valuable addition to GCHQ in meeting the demands of an integrated intelligence and security mission now and in the future. They bring personal knowledge, particular skills and expertise into GCHQ and, by their presence, help to strengthen relationships and promote greater understanding at all levels between the respective organisations.

2. GCHQ's policy for such staff with access to GCHQ systems and data consists of two parts. Part I explains the need for such a policy and outlines the different aspects that it covers. Part II conveys the detail of the policy and itself constitutes a Code of Conduct which both the member of staff on loan and the local GCHQ Business Unit Head are requested to read and sign to indicate that they agree to abide by it.

## **II. Why Do We Need a Policy?**

3. Staff on loan to GCHQ enjoy a privileged position within the department. Their work often brings them into contact with sensitive information that they would not normally be party to at their parent organisation and as such this brings with it certain responsibilities for both the individual and GCHQ as a whole. A clear understanding of these at the beginning of the period of loan will help to ensure a successful tour for all concerned.

## **III. To whom does it apply?**

4. It applies to all members of staff on loan to GCHQ with access to systems and/or data. For the most part, they work here for a limited period only, although for some the period may be much longer. The spirit of the policy also applies to members of the military unit embedded in GCHQ and the members of the Armed Forces who are not part of that unit, although they are governed by separate administrative arrangements.

## **IV. Policy Statements**

5. The detail of GCHQ's Policy for staff from the aforementioned agencies and OGDs working on GCHQ systems and data is encapsulated within the attached Code of Conduct (Pt II).

6. The Code applies in full to the period of the loan and afterwards, when such staff leave GCHQ, in respect of continuing to protect knowledge about GCHQ, its sources, methods and relationships.

7. It set outs clearly what the member of staff can expect of GCHQ in terms of the wherewithal to do their job properly and, equally, what GCHQ expects of the individual in the day-to-day execution of their duties. The Code covers the following aspects in greater detail:

- *Acting as a member of the GCHQ team*
- *Declaration of status inside & outside GCHQ*
- *Access to data, including that which GCHQ does not own*
- *Privileged access to information*
- *Respecting GCHQ's need for secrecy*
- *Working with external customers, foreign partners, collaborating Agencies etc*
- *Representing GCHQ's interests*
- *Protecting our sources and methods*
- *Conflict of Interests*
- *The continuing obligation after leaving GCHQ not to reveal details of sources, methods and relationships*
- *Deriving maximum benefit for both organisations from the period spent working at GCHQ*

# **Code of Conduct for Staff from UK Intelligence and Security Agencies and OGDs (Part II)**

## **I. Introduction**

1. Welcome to GCHQ. Staff on loan to GCHQ from other government departments (OGD), including the UK's intelligence and security agencies and other UK customer organisations, are a welcome and valuable addition to GCHQ in meeting the demands of an integrated intelligence and security mission now and in the future. They bring personal knowledge, particular skills and expertise into GCHQ and, by their presence, help to strengthen relationships and promote greater understanding at all levels between the respective organisations.
2. While on loan here you will enjoy a privileged position within GCHQ. Your work will often bring you into contact with sensitive information that you would not normally be party to at your parent organisation and as such this brings certain responsibilities for both you and GCHQ as a whole. A clear understanding of these at the beginning of your period on loan will therefore ensure a successful outcome for both you and us.
3. This is why we have produced this Code of Conduct which complements, and should be read in conjunction with, Part I of GCHQ's Policy for Staff from OGDs with access to systems and data. In essence, the Code sets out the specifics of our policy and applies in full to the time you spend working with us and afterwards in part, when you leave us, in respect of continuing to protect sensitive information and knowledge about GCHQ, its sources, methods and relationships.
4. Please read the Code carefully and sign it to indicate that you understand the need for such a Code and agree to abide by it. Once you arrive in post at GCHQ the Head of your Business Unit (BU) will meet you and also sign it as part of the induction process.

## II. The Code

### i) What you can expect from GCHQ

#### ➤ **Access to GCHQ's data**

5. GCHQ will endeavour to treat you in the same way it treats all its employees with respect to your work-related duties. In principle we will supply you with all the tools necessary for you to do your job properly, including access to relevant database information, unless particular sensitivities prevent it. However, in keeping with all other GCHQ staff, the 'need to know' rule will continue to apply to you in GCHQ as it does in your parent organisation, and therefore you will not be given blanket access to information, neither by means of IT nor by across-the-board attendance at meetings, briefings etc. Arrangements put in place for you to do your work will remain for as long as you need them and will be withdrawn by your local line management when no longer required.
6. As with all other GCHQ employees, if you are working away from GCHQ at any time your location, means of communication and local security arrangements will also be a factor in deciding what information you will be given access to.

[REDACTED]

7. [REDACTED]

8. [REDACTED]

#### ➤ **Access to other non-GCHQ data**

9. If there is a need for you to access other data or material which GCHQ does not own, the permission of the originating organisation will have to be obtained first. This applies to both Sigint and non-Sigint data / reports / assessments etc. from any of the 5 Eyes partners. A request for blanket access is not an appropriate option but it is envisaged that access to a particular line of material will only need to be requested once for an individual. Although it is unlikely, please appreciate that on occasions this may be refused for reasons of sensitivity. If this happens, your BU Head will endeavour to find an alternative solution on your behalf.

#### ➤ **Declaring your status as a secondee inside & outside GCHQ**

10. If the nature of your work involves contact with individuals or organisations outside GCHQ (including any foreign partner contacts), your local line management may, with your consent, declare your status to them and identify your parent organisation before contact is made. This will avoid any embarrassment that might ensue from a contact believing that you are a permanent employee of GCHQ and consequently imparting information to you which they might not otherwise have chosen to do.
11. For the same reason your status as a secondee will similarly be declared to those within GCHQ with whom you work. You should also reflect your status

as a secondee in any 'point of contact' details listed on your BU's webpages, in your e-mail signature block and in the GCHQ phone directory [REDACTED]. Throughout the period on loan you and your BU Head will need to ensure that your internal and external contacts remain aware of your status, especially when a change of incumbent takes place.

## ii) What GCHQ expects from you

### ➤ *You are one of us*

12. You are an integrated member of the team and should conduct yourself as a member of GCHQ. In common with your colleagues this means complying with the same range of GCHQ practices and culture that they do. These include everything from strict adherence to the rules laid down by the STRAP system and GCHQ's Compliance Documentation to acting in accordance with GCHQ's Values and observing accepted office etiquette. If in doubt about how to proceed on a particular matter, your colleagues will be happy to assist.

### ➤ *Privileged access to information*

13. During your period on loan you will have privileged access to GCHQ and partner information and data and will inevitably see much which is not directly related to your work and is only intended for internal GCHQ consumption. Any such information should not be passed outside GCHQ in any shape or form.

### ➤ *Respecting GCHQ's need for secrecy*

14. We will endeavour to ensure that you are not placed in an awkward position by exposing you to information to which you are not entitled to have access. However, should this ever happen, please do not pursue or investigate further and report the incident to your local management immediately.

### ➤ *Working with external contacts*

15. All work related business and communications with external contacts should only be conducted within the same authorised channels used by your colleagues. You may retain accounts on e-mail systems or databases at your parent organisation but may only access them from GCHQ for administrative purposes, or for keeping up with developments there. You may only use them for operational activities where there is a business need to do so which has been agreed with your BU Head.

### ➤ *Representing GCHQ's interests*

16. When dealing with external contacts, please remember that you are a member of GCHQ and as such should primarily represent GCHQ's interests. If there is a need to draw on any other views or interests as a result of work in your parent or any other organisation, you must make this clear and where appropriate emphasise that those views may not reflect official GCHQ thinking on whatever the issue at hand may be.

➤ ***Protecting our Sources and Methods***

17. Where your work does involve contact with others outside GCHQ, you should not reveal any information you have been privy to other than that which is normally discussed as a matter of course between external parties and others in your immediate work area. Except in specific, job-related circumstances, which must be agreed in advance by your BU Head, you must not otherwise disclose information or details about GCHQ's sources, methods, or relationships.

➤ ***Conflict of Interest***

18. In any loan / host Department arrangement it is a fact of life that situations can arise in which a sense of divided loyalties may be experienced (by either party). The cause of such problems can be many and varied; a difference of opinion over policy, approach, the correct course of action to take in a particular situation, and so on. Regardless of whether such feelings are justified or simply the result of a misunderstanding, the key to resolving problems of this kind is immediate, frank and open discussion between all concerned.

19. We would therefore ask both parties to adopt this approach and, in the case of staff on loan, to please raise the issue with GCHQ in the first instance. If difficulties remain after discussion has run its course, the issue should be escalated within GCHQ and pursued as a matter of urgency until the matter has been resolved amicably.

➤ ***After you leave us***

20. In accordance with the provisions of the Official Secrets Acts (1911-1989) the obligation not to reveal information, documents or articles relating to security or intelligence, which includes details about GCHQ's sources, methods, or relationships, continues after you have left GCHQ and will continue after you have left your home Department. We do, however, expect you to draw on the knowledge and experience you will have gained by working with us and to make the most of future opportunities where you believe GCHQ can be of assistance to appropriately cleared colleagues in your own or other organisations when you return to your home Department. When such opportunities arise you should not attempt to represent GCHQ's capabilities in any way, but seek to put interested parties in contact with the appropriate area of GCHQ. The reason for this is that apart from the risk of inadvertently compromising those capabilities, Sigint is a fast-moving business and the most current and authoritative information will always be available in GCHQ itself.

### **III. Further Guidance / Complaints**

21. We very much hope that you enjoy the time you spend with us and everybody in GCHQ will be only too happy to assist you in settling in fast and becoming part of the Team. If you do have any cause for concern, please consult your local management in the first instance.

22. Once you arrive in post at GCHQ the Head of your Business Unit (BU) will meet you and also sign this Code of Conduct to indicate that you have both understood it and have agreed to abide by it. Each of you should retain a copy for future reference. Copies should be stored locally for the duration of the posting.

23. The relevant policy team should also be notified when a new Integree has signed this agreement for our records (email [REDACTED]).

Staff member

GCHQ BU Head

Name .....

Name .....

Signature .....

Signature .....

Parent Organisation .....

BU .....

Date .....

Date .....



Dear Mr Webber,

In the IPT's letter of 13 April 2017 the Tribunal asked for a response in open "*based on assumed facts whether, if a transfer of BCD and/or BPD to another agency or organisation, including a foreign agency, had taken place, they have regarded it as within their remit, and confirm that, in that event, they would have provided active oversight.*"

As you know, there was a procedural hearing in this case on Friday 5 May 2017. Your letter of 27 April 2017 was considered at that hearing. Representations were made by the Claimant to the effect that the Tribunal should ask the Commissioners to provide some further information. That is the purpose of this letter.

Two issues arise.

First, the Claimant suggested that the use of assumed facts was not necessary in the case of sharing by GCHQ with industry partners.

GCHQ has disclosed policy documentation indicating that it shares "*sets of raw Sigint Data with commercial partners and suppliers contracted to develop new systems and capabilities for GCHQ.*" The document, a copy of which is attached, also outlines the processes that GCHQ follows prior to releasing data of this sort to industry partners.

In a Response to a Request for Further Information, GCHQ has provided the following relevant information:

"The position regarding GCHQ is that 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. [...]"

"... when operational data (which could in theory include BCD / BPD) is shared with industry partners, it is usually retained within GCHQ premises in the UK. When it is not stored within GCHQ premises, the storage will be accredited by GCHQ. In all such cases the storage has been within the UK."

The Claimant's skeleton argument of 23 February 2017 sets out the Claimant's case as to what has been placed in the public domain and avowed:

"It is common ground that GCHQ disclose entire databases of "*raw sigint data*" to "*industry partners*" who have been "*contracted to develop new systems and capabilities for GCHQ*" [3/476]. It is avowed that there are "*frequent releases of routine sets of raw Sigint data to industry partners*" [3/476]. When this occurs, there appear to be few safeguards. For example, there appears to be no requirement for each search to be explained and justified in writing. Security clearance is required only "*wherever possible*" [3/476]."

The Claimant queries whether there has in the past been oversight of industry sharing by the Commissioners. In particular, they wish to know whether the Commissioners carried out an audit of the transfer of data to industry partners and audited the use made of the transferred data. Have the Commissioners visited industry partners in order to check the use made of bulk data that has been shared and transferred or to which access has been given, and the systems and safeguards applied? For example, the Claimant has served a Request for Information asking:

"15. Has the Intelligence Services Commissioner or any other oversight body ever audited the sharing of BCD and/or BPD with... industry partners?"

- (a) If so, how was the audit conducted?
- (b) What were the results of that audit?
- (c) Did the audit examine the actual queries and use made of transferred data, and its storage and destruction?"

The dates, frequency and circumstances of any audit will also be relevant, as well as the procedures used to conduct the audit and information about the depth of the audit. How often do the Commissioners visit 'industry partners'? What work is carried out to audit their use of BCD/BPDs? What sort of searches and investigations are carried out?

The Tribunal would be grateful for the Commissioners' assistance with an open response to these queries as soon as possible.

Secondly, in the letter of 13 April, the Tribunal asked whether the Commissioners would have provided "*active oversight*". We note that the Commissioners' response is in terms of matters being within the scope of the Commissioners' oversight. It does not deal with whether "*active*" oversight would have been carried out.

It may be relevant to know whether the Commissioners have taken active steps to implement oversight within their remit. If a matter is within the scope of the Commissioner's remit but has never been in fact audited and no other form of active oversight has been carried out, it may be suggested by the Claimant that the oversight provided to date has not been adequate. The Tribunal would therefore be grateful for a more detailed open response to the question so that the actual application of any oversight can be understood, even if in necessarily general terms.

This letter is served pursuant to section 68(2) of RIPA 2000.

The hearing on sharing is listed for Monday 5 June 2017 and the Claimant's skeleton argument is due on Monday 15 May. We would therefore appreciate as prompt a response as possible.

Yours etc.



(c) crown copyright

Catalogue Reference:HW/80/4

Image Reference:1

**Department**

HW

**Series**

80

**Piece**

4

TOP SECRET

BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

5 March 1946

\* \* \*  
\*\*\*  
\*

TOP SECRET

# TOP SECRET

## OUTLINE OF

### BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

1. Parties to the Agreement
2. Scope of the Agreement
3. Extent of the Agreement - Products
4. Extent of the Agreement - Methods and Techniques
5. Third Parties to the Agreement
6. The Dominions
7. Channels between U. S. and British Empire Agencies
8. Dissemination and Security
9. Dissemination and Security - Commercial
10. Previous Agreements
11. Amendment and Termination of Agreement
12. Activation and Implementation of Agreement

TOP SECRET

# TOP SECRET

## BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

### 1. Parties to the Agreement

The following agreement is made between the State-Army-Navy Communication Intelligence Board (STANCIB) (representing the U. S. State, Navy, and War Departments and all other U. S. Communication Intelligence<sup>1</sup> authorities which may function) and the London Signal Intelligence (SIGINT) Board (representing the Foreign Office, Admiralty, War Office, Air Ministry, and all other British Empire<sup>2</sup> Communication Intelligence authorities which may function).

### 2. Scope of the Agreement

The agreement governs the relations of the above-mentioned parties in Communication Intelligence matters only. However, the exchange of such collateral material as is applicable for technical purposes and is not prejudicial to national interests will be effected between the Communication Intelligence agencies in both countries.

---

<sup>1</sup>Throughout this agreement Communication Intelligence is understood to comprise all processes involved in the collection, production, and dissemination of information derived from the communications of other nations.

<sup>2</sup>For the purposes of this agreement British Empire is understood to mean all British territory other than the Dominions.

TOP SECRET

3. Extent of the Agreement - Products

(a) The parties agree to the exchange of the products of the following operations relating to foreign communications:<sup>3</sup>

- (1) collection of traffic
- (2) acquisition of communication documents and equipment
- (3) traffic analysis
- (4) cryptanalysis
- (5) decryption and translation
- (6) acquisition of information regarding communication organizations, practices, procedures, and equipment

---

<sup>3</sup>Throughout this agreement foreign communications are understood to mean all communications of the government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include communications of a foreign country which may contain information of military, political, or economic value. Foreign country as used herein is understood to include any country, whether or not its government is recognized by the U. S. or the British Empire, excluding only the U. S., the British Commonwealth of Nations, and the British Empire.

TOP SECRET



# TOP SECRET

(b) Such exchange will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

## 4. Extent of the Agreement - Methods and Techniques

(a) The parties agree to the exchange of information regarding methods and techniques involved in the operations outlined in paragraph 3(a).

(b) Such exchange will be unrestricted on all work undertaken, except that upon notification of the other party information may be withheld by either party when its special interests so require. Such notification will include a description of the information being withheld, sufficient in the opinion of the withholding party, to convey its significance. It is the intention of each party to limit such exceptions to the absolute minimum.

## 5. Third Parties to the Agreement

Both parties will regard this agreement as precluding action with third parties<sup>4</sup> on any subject appertaining to Communication Intelligence except in accordance with the following understanding:

---

<sup>4</sup>Throughout this agreement third parties are understood to mean all individuals or authorities other than those of the United States, the British Empire, and the British Dominions.

# TOP SECRET

- (a) It will be contrary to this agreement to reveal its existence to any third party whatever.
- (b) Each party will seek the agreement of the other to any action with third parties, and will take no such action until its advisability is agreed upon.
- (c) The agreement of the other having been obtained, it will be left to the party concerned to carry out the agreed action in the most appropriate way, without obligation to disclose precisely the channels through which action is taken.
- (d) Each party will ensure that the results of any such action are made available to the other.

## 6. The Dominions

- (a) While the Dominions are not parties to this agreement, they will not be regarded as third parties.
- (b) The London SIGINT Board will, however, keep the U. S. informed of any arrangements or proposed arrangements with any Dominion agencies.
- (c) STANCIB will make no arrangements with any Dominion agency other than Canadian except through, or with the prior approval of, the London SIGINT Board.
- (d) As regards Canada, STANCIB will complete no arrangements with any agency therein without first obtaining the views of the London SIGINT Board.
- (e) It will be conditional on any Dominion agencies with whom collaboration takes place that

SECRET

# TOP SECRET

they abide by the terms of paragraphs 5, 8, and 9 of this agreement and to the arrangements laid down in paragraph 7.

## 7. Channels Between U. S. and British Empire Agencies

(a) STANCIB will make no arrangements in the sphere of Communication Intelligence with any British Empire agency except through, or with the prior approval of, the London SIGINT Board.

(b) The London SIGINT Board will make no arrangements in the sphere of Communication Intelligence with any U. S. agency except through, or with the prior approval of, STANCIB.

## 8. Dissemination and Security

Communication Intelligence and Secret or above technical matters connected therewith will be disseminated in accordance with identical security regulations to be drawn up and kept under review by STANCIB and the London SIGINT Board in collaboration. Within the terms of these regulations dissemination by either party will be made to U. S. recipients only as approved by STANCIB; to British Empire recipients and to Dominion recipients other than Canadian only as approved by the London SIGINT Board; to Canadian recipients only as approved by either STANCIB or the London SIGINT Board; and to third party recipients only as jointly approved by STANCIB and the London SIGINT Board.

## 9. Dissemination and Security - Commercial

STANCIB and the London SIGINT Board will ensure that without prior notification and consent of the other party in each instance no dissemination of information derived from Communication Intelligence sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

# TOP SECRET

## 10. Previous Agreements

This agreement supersedes all previous agreements between British and U. S. authorities in the Communication Intelligence field.


## 11. Amendment and Termination of Agreement

This agreement may be amended or terminated completely or in part at any time by mutual agreement. It may be terminated completely at any time on notice by either party, should either consider its interests best served by such action.


## 12. Activation and Implementation of Agreement

This agreement becomes effective by signature of duly authorized representatives of the London SIGINT Board and STANCIB. Thereafter, its implementation will be arranged between the Communication Intelligence authorities concerned, subject to the approval of the London SIGINT Board and STANCIB.

For and in behalf of the  
London Signal Intelligence Board:

  
Patrick Marr-Johnson  
Colonel, British Army  
General Staff

For and in behalf of the  
State-Army-Navy Communication Intelligence Board:

  
Hoyt S. Vandenberg  
Lieutenant General, GSC  
Senior Member

5 March 1946

TOP SECRET