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 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?

<u>Response to requests 3-5</u>

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.[1] 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*

[1] 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 integrees 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