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

THE RESPONDENTS' AMENDED RESPONSE TO THE CLAIMANTS' SUPPLEMENTAL REQUEST FOR FURTHER INFORMATION AND DISCLOSURE DATED 10 JUNE 2016

This Amended Response provides further information (underlined and in bold) in respect of certain of the Claimant's requests. The provision of this Amended Response follows requests by Counsel to the Tribunal to provide in some cases more detailed responses to requests and in other cases to disclose into OPEN responses previously given in CLOSED. Counsel to the Tribunal has also revisited all earlier documentation referred to in the Request for Further Information; he has made some further consequential requests for disclosure, which are referred to below.

The Respondents note that a significant number of the requests (i.e. those numbered 11 to 47) relate to documents provided to the Claimant on 11 and 12 April 2016. However, no requests were made about them until 10 June 2016. As a consequence the Respondents are being asked to provide significant amounts of further information unnecessarily close to, and at the time when the Respondents are preparing for, the substantive hearing on 25-29 July 2016. The Respondents rely generally on this fact in support of the contention, which is also made for the specific reasons given below, that it would be disproportionate to be required to respond to a number of the relevant requests.

In response to the concern raised in the preamble at page 2 of the RFI, the Respondents can say that redactions have been marked throughout. For the avoidance of doubt, the colon at

the end of paragraph 9.2 of Exhibit O is present in the CLOSED version of the document and no material has been redacted between paragraphs 9.2 and 9.3 of that document.

Correspondence between Home Office and Sir Swinton Thomas (Interception of Communications Commissioner) in 2004

1. Do the Respondents now accept that the bulk transfer of data from CSPs to the Agencies engages Article 8 ECHR, and EU data protection law, even if the data does not contain the real name of the person?

Yes.

2. Do the Respondents now accept that data which can be deanonymised by the Agencies (e.g. a database containing phone numbers but not subscriber names) is personal data, and engages Article 8 ECHR?

Yes.

3. Does the Commissioner now accept the same?

This is not an appropriate Request for Further Information. It concerns the opinion of the Commissioner, who is not a Respondent to the claim, regarding the law. The Respondents do not respond to it.

4. If so, when did the Respondents and the Commissioner first accept that the transfer of such data engages Article 8 ECHR and is personal data? Please disclose all relevant documents evidencing the change in position of (a) the Respondents; and (b) the Commissioner.

In relation to the request concerning the Commissioner, the Respondents repeat their response to Request 3.

In relation to the request about the Respondents themselves, the request is irrelevant. The engagement or otherwise of Article 8 ECHR is a matter of law, not a matter of opinion.

5. Was the Commissioner's attention drawn to section 1(1) of the Data Protection Act 1998 or Article 2(a) of the Data Protection Directive? If so, when? Please provide copies of the relevant documents.

The Respondents have no record of having themselves drawn these matters to the Commissioner's attention. The Respondents are unable to say whether or not these matters were drawn to the Commissioner's attention by members of his office or by anyone else.

6. Please confirm that all correspondence between the Interception of Communications Commissioners and the Respondents relating to Bulk Personal Datasets and s.94 TA 1984 has now been disclosed, including the results of any inspections or audits.

This request is still under consideration. The Respondents aim to be able to respond to it on or before the hearing on 7 July 2016.

This is not confirmed. The Respondents have complied with the disclosure orders made by the Tribunal and have provided further disclosure in response to particular requests that have been made both by the Tribunal and by Counsel to the Tribunal. The scope of disclosure envisaged in this request, by contrast, is far greater in scope, and, for the avoidance of doubt, such disclosure has not been given.

GLD letter of 11 April 2016

7. Please provide the December 2014 and December 2015 IOCCO Security Service inspection report and the preceding reports referred to.

Disclosure of the 2014 and 2015 reports in OPEN would damage national security. The Respondents are however actively considering the extent to which they can provide a redacted version and/or a gist of the reports in OPEN. They will provide that as soon as possible.

Redacted versions of extracts from the 2014 and 2015 inspection reports will be disclosed in OPEN, together with similarly redacted extracts from the preceding reports for the years 2011-2013. As the extracts from the 2011-2013 reports demonstrate, in previous years the Commissioner had not asserted that this practice was not compliant.

8. Please provide a copy of the briefing notes to the Home Secretary and the Home Secretary's response.

Copies of the Home Secretary's letters to the Security Service of 27 March 2015 and 3 June 2015 are provided. The balance of this correspondence cannot be disclosed in OPEN without damaging national security. The Respondents are however actively considering the extent to which they can provide a redacted version and/or a gist of the documents in OPEN. They will provide that as soon as possible.

Redacted copies of the letters from the Security Service to the Home Secretary will now also be disclosed in OPEN.

9. What is the factual basis for the assertion that use of an independent DP is not possible

for reasons of security, in circumstances where an independent DP is now always used in cases involving sensitive professions.

The factual considerations underlying the Security Service's position that the use of independent DPs for all CD requests has not been practicable are:

(a) The volume of CD requests that MI5 processes and the consequential volume of work for DPs considering requests, and

(b) The particularly sensitive nature of some of MI5's investigations and the consequential need to preserve "need to know" in relation to such investigations.

Further, and in particular as to (a) above, to the extent that a DP would not be familiar with a particular investigation, then the need to brief him/her on the underlying facts and context for a request will be that much greater, resulting in additional levels of work and time involved in the authorisation process. DPs are key operational managers with a range of functions within MI5, and additional time spent on authorisations would necessarily impact on their ability to fulfil those other functions.

10. Please provide a copy of the correspondence with the Commissioner expressing concerns at the Security Service's current practices around the use of DPs.

This correspondence cannot be disclosed in OPEN without damaging national security. The Respondents are however actively considering the extent to which they can provide a redacted version and/or a gist of the documents in OPEN. They will provide that as soon as possible.

Redacted copies of this correspondence will now be disclosed in OPEN.

Closed Response to RFI dated 15 January 2016

11. Generally: Responses have only been provided from 1 June 2014 onwards. Please provide responses to the queries from June 2005 onwards. It is not sufficient to only answer queries within a year of issue, because the relevant use of BPD and BCD was deliberately concealed from the public, including any information about safeguards, errors or misuse.

This relates to the CLOSED response to Request 12 in the Claimants' 15 January 2016 Request for Further Information.

The request is refused. It is disproportionate to provide responses to the said queries from June 2005 onwards. In circumstances where (i) the request relates to an 11-year period; (ii) the Tribunal has already ruled that the appropriate timeframe for disclosure of "events", as

opposed to safeguards, is 1 June 2014 onwards, and (iii) the Tribunal can, as in previous cases, assess the adequacy of safeguards by reference to those safeguards themselves, without information of the kind requested.

12. Security Service BPD errors: Please identify the nature and content of the deleted dataset, how long it was held, how often it was accessed or used and why it has now been deleted. Please state the exact nature of the individual non-compliance by staff members and the outcome of the disciplinary procedures.

The Security Service is unable to identify in OPEN the nature and content of the deleted dataset as to do so would damage national security. The dataset was first acquired in February/March 2015 and was held by the Security Service until it was deleted in February 2016. The Security Service is unable to answer, in OPEN, the request relating to how many times it was accessed/used as to do so would damage national security. The dataset was deleted as it was decided that it ceased to be necessary and proportionate to retain it. The non-compliance was that it was not appreciated, at the time of acquisition, that the nature of the data was such that it constituted "bulk personal data". Accordingly the dataset was not made subject to the BPD acquisition process. No disciplinary action has been taken.

13. Security Service BCD errors: Please give full and precise particulars of the necessity and proportionality errors and disclose the documents setting out the errors and the action taken on their discovery.

The Respondents cannot respond to this request in OPEN without causing damage to national security. Further, and in any event, the request is irrelevant and disproportionate, as it seeks information which is not required in order for the Tribunal to determine the claim.

For the avoidance of doubt, these documents have in any event been provided to Counsel to the Tribunal.

14. SIS BPD errors: Please identify the type and content of the mistakenly ingested datasets, how long they were held, how often they were accessed or used and whether their use has now been authorised. Please unredact the withheld part of (a)(i). Please state the exact nature of the individual non-compliance by staff members and the outcome of the disciplinary procedures.

Both of the datasets were biographical datasets. Both datasets have since been correctly ingested and authorised.

The withheld part of (a)(i) read: "This was possible because of an ambiguity within the internal workflow IT system. SIS have since made changes which prevent this from happening again."

As noted in the Closed Response to RFI, the errors were not ascribable to any staff member's failure to comply. Accordingly no disciplinary action was taken.

Closed Response

15. Paragraph 108: Please identify the alleged safeguards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

16. As to the use of experiments (e.g. paragraph 123), please identify the extent to which such experimental activity takes place, whether external contractors are given access to bulk datasets, and whether such use is and has been fully audited by the Commissioners and whether each search or algorithm developed is subject to approval and a written justification prepared before use, and identify the restrictions preventing the viewing of material being used for experimental use.

This request is still under consideration. The Respondents aim to be able to respond to it on or before the hearing on 7 July 2016.

The SIA conduct experimental activity using bulk personal data, including large scale projects, involving the testing of a hypothesis or trialling a new application. This experimentation explores the benefit of the further development of a new tool or technique, to be used in support of the Respondents' statutory functions. Experiments may involve an element of cross-Agency collaboration. Access to any experimental activity is limited to a small number of specialist users and all such staff, including external contractors, receive appropriate specialist training and may be subject to additional security clearance. All experimental activity is subject to written justification prior to work commencing and all use of bulk personal data is overseen by the Intelligence Services Commissioner.

17. How many BPDs have been deleted as a result of an internal review process?

The Respondents cannot respond to this request in OPEN without causing damage to national security. Further, and in any event, the request is irrelevant and disproportionate, as it seeks information which is not required in order for the Tribunal to determine the claim.

Over the period from January 2010 to date, all 3 agencies have deleted BPDs as a result of internal review processes. The number of BPDs deleted by MI5 over this period equates to 75% of its current BPD holdings. The figures for GCHQ and SIS are 51% and 10% respectively. It should be added, however, that there are no GCHQ deletion records

available for 2010 or 2012, and no definitive deletion records are available for SIS prior to 2012.

18. How many BPDs have been deleted as a result of an opinion expressed by a Commissioner?

No BPDs have been deleted as a result of an opinion expressed by a Commissioner.

19. Footnote 6: Please explain why the use of section 22 RIPA to authorise access to or use of BCD was not disclosed in the Open Response, identifying the alleged national security reason why it was not disclosed.

This request is irrelevant to the issues in the case. The Respondents accordingly do not respond to it.

Closed Exhibits

20. Exhibits E, P and R: The entire exhibits have been redacted, without even a title. Please disclose the document, or gist it.

Exhibit E is the Security Service's Security Operating Procedures for Privileged Users with access to the Security Service's IT Systems and Services. The Security Service is actively considering the extent to which they can provide this document in OPEN and they will provide that, subject to appropriate redactions on the grounds of national security, as soon as is practicable.

A redacted OPEN version of this document will be served.

Exhibit P is at pages 167 to 174 of exhibit "GCHQ1" to the GCHQ witness statement.

Exhibit R cannot be disclosed in OPEN without causing damage to national security.

21. Exhibit H: Please disclose the redacted timescales for acquisition and use, the redaction following the requirement for appropriate authorisation, the redactions detailing permitted use and the redactions about data sharing with SIA partners.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

22. Exhibit H: External Oversight: Please disclose all documents recording consideration within the Agencies and the other Respondents as to the scope, adequacy and potential changes to external oversight.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

This request is refused. It is not accepted that this material is relevant to the issues before the Tribunal. Further or in the alternative, providing such disclosure would not be possible without causing damage to national security and would in any event be entirely disproportionate.

23. Exhibit H, Corporate Risk: the gist concerning bulk financial information appears to be unnecessary and designed to minimise embarrassment rather than protect national security. Please disclose.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

24. Exhibit I: Please disclose the redacted passages in paragraphs 5.1.1, 7.3.2, 8.0.4-5, 9.1 and 9.3.4 all of which appear to set out relevant safeguards, or caveats on safeguards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be served.

25. Exhibit J: Please disclose the redacted passages in paragraphs 4-7 and 9-11 all of which appear to set out relevant safeguards, or caveats on safeguards.

Please clarify this request. Exhibit J does not contain numbered paragraphs.

It is understood that this request is intended to refer to Exhibit O. An amended OPEN version of this document will be served.

26. Exhibit S: Please disclose the redacted or gisted passages in paragraphs 2.4, 3.18, 4.3, 4.3.5, 4.3.6 and 4.3.8 all of which appear to set out relevant safeguards, or caveats on safeguards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be served.

27. Exhibit T: Please disclose the redacted or gisted passages in paragraphs 2 and 4 all of

which appear to set out relevant safeguards, or caveats on safeguards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be served.

Pre-2014 Disclosure

28. Document 1: Section VI, footnote 1 cross-refers to a 1999 paper on Databases written for the IOCA and ISA Commissioners. Please disclose.

This document cannot be disclosed in OPEN without damaging national security. The Respondents are however actively considering the extent to which they can provide a redacted version and/or a gist of the documents in OPEN. They will provide that as soon as possible.

Redacted OPEN versions of these documents will be provided.

29. Document 3, page 9: Please disclose the guidance for sharing operational data with a company.

This document cannot be disclosed in OPEN without damaging national security. The Respondents are however actively considering the extent to which they can provide a redacted version and/or a gist of the documents in OPEN. They will provide that as soon as possible.

A redacted OPEN version of this document will be provided.

30. Document 9: Please disclose the worked examples. It is not possible to understand whether there are adequate and proper safeguards in practice without some disclosure of details of usage.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

31. Document 10: This policy guidance should be disclosed in full. Guidance about legal authorisation methods and safeguards is not secret.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

32. Document 11: The gist provided is entirely inadequate. The source document should be disclosed. Or if not possible, the nature of the workshops, the reasons for them, and any concerns that were addressed in them or disclosed by them ought to be disclosed.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

33. Document 13: Please disclose document in full. The gist is inadequate. What was the previous audit trail? Why were new procedures requires [*sic*] to make the audit trail adequate? What changed? Which section of the Service was failing to keep a proper audit trail? How many people were affected? How was the problem discovered?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

The purpose of the change in procedure described in the Loose Minute was unrelated to the internal audit process, which was unchanged as between the two procedures.

34. Document 14. As document 11. Was there evidence that analysts were not properly confining the time periods of their requests? If so, how was this problem discovered? How many people were affected?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

This document was written following technical improvements to the electronic system for making CD requests. The purpose of this document was to update staff on the functionality of the system and the importance of continued compliance. It is not the case that this document was written in response to any evidence of non-compliance.

35. Document 15: Disclose document in full. There is no good reason for a partial gist to be provided.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

36. Document 16: Disclose redacted item(s) in table of contents. From the substance of the document, this appears to be a reference to "Collateral Intrusion".

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be served.

37. Document 16: Disclose Annex A. If standard form wording and justifications are used, this is a relevant matter in considering whether the systems and safeguards provided are adequate.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Annex A of this document cannot be disclosed without causing damage to national security. For the avoidance of doubt, however, Annex A does not provide standard wording or justifications. Rather, it provides good examples of justifications drawn from actual cases that are intended to assist officers in formulating justifications in their own work.

38. Document 17: Annex B. As document 16.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Annexes A and B of this document cannot be disclosed without causing damage to national security. For the avoidance of doubt, however, Annexes A and B do not provide standard wording or justifications. Rather, they provides good examples of justifications drawn from actual cases that are intended to assist officers in formulating justifications in their own work.

39. Document 18: As document 16 and 17.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Annexes A and B of this document cannot be disclosed without causing damage to national security. For the avoidance of doubt, however, Annexes A and B do not provide standard wording or justifications. Rather, they provides good examples of justifications drawn from actual cases that are intended to assist officers in formulating justifications in their own work.

40. Document 19: As document 16 and 17.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Annexes A and B of this document cannot be disclosed without causing damage to national security. For the avoidance of doubt, however, Annexes A and B do not provide standard

wording or justifications. Rather, they provide good examples of justifications drawn from actual cases that are intended to assist officers in formulating justifications in their own work.

41. Document 21: Database newsletters:

(a) Please identify how each instance of misuse of the dataset referred to was discovered and what action was taken against each individual responsible.

Each instance of non-compliance referred to in this document was identified by the SIS audit team. The individuals concerned were all required to confirm that they had re-read the database Code of Practice and were warned that any future incidents may lead to disciplinary action. In each case, the individual's line manager was informed.

(b) Please provide the original text of the gist *"for personal reasons"*, so that the nature and extent of the misuse can be understood. This gist appears to have been introduced to avoid embarrassment at the disclosure of misconduct, not for a genuine reason of national security.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

The original text cannot be given for national security reasons. The gist that can be given is "for personal reasons related to clearance". See also the witness statement of the SIS witness at paragraph 62. An amended version of document 21 has been provided.

(c) How many searches have been made for public figures without a proper operational need?

The Respondents cannot respond to the request in OPEN without causing damage to national security.

Between 2009 and 2013, there were three searches of high profile individuals (by three different users) that were not operationally justifiable. There have been none since 2013.

There were 17 searches of high profile individuals (by five different users) between 2009 and 2011 which may not have been operationally justifiable. However, SIS has no formal record of conversations with the users or their line managers and it is therefore now not possible to ascertain whether they were in fact operationally justifiable.

(d) As at 2011 and 2012, was there any requirement to record the reasons for a search, or any form of documented justification?

As at 2011 and 2012, there was no mandatory requirement to record the reasons for a search. However, users did as a matter of practice frequently record their reasons for searches to assist in responding to audit justification requests and enquiries by the Intelligence Services Commissioner.

Open Disclosure in Response to RFI

42. Document 7, footnote 1: Please provide copy of correspondence between GCHQ and Cabinet Office.

The terms referred to were agreed orally. There was no such correspondence.

43. Document 15: Please disclose redacted material in footnotes 2 and 3 defining metadata and content. Please disclose (or gist) examples of intrusion assessments and the redacted passages relating to 'corporate risk'.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be provided.

44. Document 17: Disclose redacted passages in Sections B-E which appear to set out safeguards or caveats on safeguards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be provided.

45. Document 31: Please disclose redacted parts of document, which set out safeguards and procedures and report on compliance standards.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be provided.

46. Document 34 and 35: Please disclose redacted parts of document.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

An amended OPEN version of this document will be provided.

47. Document 44: Please provide the documents recording the Commissioner's analysis, views and conclusions and please disclose redacted parts of document [*sic*], which set out safeguards and procedures.

As to the request for documents, the only documents which would fall within the scope of this request are the reports produced by the Commissioner. The Respondents are currently considering whether and to what extent the said reports may be disclosed into OPEN.

As to the document request, the reference to the Commissioner in this document was not referring to any specific document where his analysis, views and conclusions were recorded. The Commissioner's analysis, views and conclusions are published in his annual reports.

As to the request to disclose redacted parts of document 44, the Respondents cannot respond to this request in OPEN without causing damage to national security.

GCHQ Witness Statement

48. Paragraphs 8-11: Does the data in BPD repositories include information obtained under section 94 TA? Is this tool made available to other government organisations, such as HMRC?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

One specific BPD obtained under the terms of section 94 has been stored in the main BPD repository. The requirement for this data ceased in August 2015 and all such data had been destroyed by October 2015. The BPD tools are not made available to other government organisations. Integrees from other Departments who are based at GCHQ may have access, but only for GCHQ purposes.

49. Paragraph 12: Does the data in BPD repositories include information obtained under section 94 TA? Is this tool made available to other government organisations, such as HMRC?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

No. See the response to request 48.

50. Paragraph 18: Does 'travel data' include locational information obtained under section 94 TA and/or under section 8(4) warrants?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

No.

51. Paragraph 24: Has GCHQ held a BPD consisting of medical records in the past? If so, please state when the BPD was obtained and deleted, the reasons for its obtaining and deletion, whether the BPD was domestic, foreign or both and the use made of it. Please disclose all relevant documents setting out the obtaining, approval, use made and deletion of the BPD. There is no national security reason for refusing to provide responses - both MI5 and MI6 have expressly denied *ever* holding a medical or health BPD. Accordingly, a NCDN response is wrong in principle.

GCHQ has not held a BPD consisting of medical records in the past.

52. Paragraph 65: Please disclose the training materials.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

The relevant sections of the AML and MLO online training packages have been set out in full in paragraphs 61 and 63 of the GCHQ witness statement. Redacted OPEN versions of the specific training for the two BPD repositories referred to in paragraph 65 will be disclosed.

53. Paragraphs 67-99: Please disclose the records of the meetings, the documents discussed at the meetings and any correspondence prior to and after the meeting.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

These meetings are not formally minuted by GCHQ. GCHQ keeps a file note for internal purposes, and there is an agreed list of actions. Correspondence after the meetings covers progress in relation to any actions agreed during the inspection.

Copies of these documents have been provided to the Tribunal and redacted OPEN versions of relevant file notes will be served.

54. Paragraph 70: Please confirm that as at December 2010, there was no requirement for analysts to record an authorised purpose, a JIC requirement or a free-text justification before each BPD search.

As at December 2010 there was a requirement for analysts to record in the tool an authorised purpose, a JIC requirement and a free-text justification before each BPD search.

55. Paragraph 73: Please provide the TDS analysis as of March 2011 demonstrating the usefulness of BPDs.

The request appears to be premised on a misreading of paragraph 73. Paragraph 73 refers to the TDS screen which would enable data to be generated on what sources of data were productive, but does not state that there was a "TDS analysis" as of March 2011 as such.

56. Paragraph 73: What audit did Sir Mark Waller carry out of the use of the BPDs, or of the proportionality of their retention and use? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

The Intelligence Services Commissioner (Sir Mark Waller in this instance) inspects BPD twice each year, selecting which BPDs he wishes to focus on from a full list of all current BPD held by GCHQ. He checks that the documentation (BPDAR) is in order, gives a good case for acquisition and retention of the dataset including necessity, proportionality and risk of collateral intrusion. He has also made clear the need for full deletion of a dataset when it is no longer required and for proper recording of the deletion. He also discusses the operational use of those BPDs he has selected, with those who own the dataset, asking questions etc. particularly around the necessity and proportionality/collateral intrusion aspects. This can be in whatever depth he desires. Thus, he looks at the overall use and purpose of the data rather than specific requests made of the data.

Sir Mark has not been given samples of the queries run against any BPD.

57. Paragraph 76: What audit did Sir Paul Kennedy carry out of the use of the BPD, or of the proportionality of its retention and use? Did Sir Paul Kennedy examine a sample of the queries made, or examine whether they were proportionate and necessary?

The nature and scope of the inspections carried out by Sir Paul Kennedy was identical to those carried out by the Intelligence Services Commissioner, as set out in the response to request 56 above.

58. Paragraph 77: What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 56.

59. Paragraph 78: What audit did Sir Paul Kennedy carry out of the use of the BPD? Did Sir Paul Kennedy examine a sample of the queries made, or examine whether they were

proportionate and necessary?

Please see the response to request 57.

60. Paragraph 79: When was the "highly sensitive and closely held dataset" obtained? Did the Commissioner express any concerns? What is the nature of the dataset? What audit did Sir Paul Kennedy carry out of the use of the BPD? Did Sir Paul Kennedy examine a sample of the queries made, or examine whether they were proportionate and necessary?

The Commissioner did not express any concerns. The Respondents are not otherwise able to respond to this request in OPEN without causing damage to national security.

The dataset was obtained in the same year. It was financial in nature. Sir Paul Kennedy did review the use of the dataset. His review consisted of an initial check that the documentation (BPDAR) was in order, gave a good case for acquisition and retention of the dataset including necessity, proportionality and risk of collateral intrusion. He discussed the operational work of the dataset with those who own the dataset, asking questions particularly around the issues of necessity, proportionality and collateral intrusion. Thus he looked at the overall use and purpose of the data rather than the specific requests made of the data.

61. Paragraph 80: What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 56.

62. Paragraphs 81-82: What was the retention period? Has this now been changed? What audit did Sir Anthony May carry out of the use of the BPD? Did Sir Anthony May examine a sample of the queries made, or examine whether they were proportionate and necessary?

The Respondents cannot respond to the request concerning the retention period in OPEN without causing damage to national security.

Otherwise, please see the response to request 56.

Sir Anthony May did review the use of the dataset(s) in question at the inspection visit. His review consisted of an initial check that the documentation (BPDAR) was in order, gave a good case for acquisition and retention of the dataset(s) including necessity, proportionality and risk of collateral intrusion. He discussed the operational work of the dataset(s) with those who own the dataset, asking questions particularly around the issues of necessity,

proportionality and collateral intrusion. Thus he looked at the overall use and purpose of the data rather than the specific requests made of the data.

63. Paragraph 83: What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 56.

64. Paragraph 84: What audit did Sir Anthony May carry out of the use of the BPDs? Did Sir Anthony May examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 57.

65. Paragraph 85-86: Please identify the nature and content of the datasets referred to. What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

The Respondents cannot respond to the request concerning the nature and content of the datasets referred to in OPEN without causing damage to national security.

The first dataset was a travel dataset. The second dataset was a biographical dataset. Sir Mark Waller did review the use of the datasets in question at the inspection visit. His review consisted of an initial check that the documentation (BPDAR) was in order, gave a good case for acquisition and retention of the datasets including necessity, proportionality and risk of collateral intrusion. He discussed the operational work of the datasets with those who own the dataset, asking questions particularly around the issues of necessity, proportionality and collateral intrusion. Thus he looked at the overall use and purpose of the data rather than the specific requests made of the data.

Otherwise, please see the response to request 56.

66. Paragraph 87: What audit did Sir Anthony May carry out of the use of the BPDs? Did Sir Anthony May examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 57.

67. Paragraphs 88-89: Please identify the nature and content of the datasets referred to. What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and

necessary?

The Respondents cannot to respond to the request concerning the nature and content of the datasets referred to in OPEN without causing damage to national security.

Otherwise, please see the response to request 56.

Sir Mark Waller conducted an inspection on 28-29 May 2014 of 3 specific datasets. They were: a commercial dataset, a communications dataset containing publicly available subscriber data and a financial dataset containing financial data with very strict rules of access. Sir Mark did review the use of the datasets at the inspection visit. His review consisted of an initial check that the documentation (BPDAR) was in order, gave a good case for acquisition and retention of the datasets including necessity, proportionality and risk of collateral intrusion. He discussed the operational work of the datasets with those who own the dataset, asking questions particularly around the issues of necessity, proportionality and collateral intrusion. Thus he looked at the overall use and purpose of the data rather than the specific requests made of the data.

68. Paragraphs 90-91: What audit did Sir Anthony May carry out of the use of the BPDs? Did Sir Anthony May examine a sample of the queries made, or examine whether they were proportionate and necessary?

Please see the response to request 57.

69. Paragraph 92: What were Sir Mark Waller's conclusions? What steps did he taken in the inspection? What audit did Sir Mark Waller carry out of the use of the BPDs? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary?

The Respondents have no record of Sir Mark Waller's conclusions in relation to these datasets. As any concerns would have been recorded, the Respondents conclude that Sir Mark Waller did not have any concerns in relation to the holding and use of these datasets.

Please see the response to request 56.

70. Paragraphs 93-94: What were Sir Mark Waller's conclusions as to the necessity and proportionality of the holding and use of this dataset? What steps did he take in the inspection? What audit did Sir Mark Waller carry out of the use of the BPD? Did Sir Mark Waller examine a sample of the queries made, or examine whether they were proportionate and necessary? What examination did Sir Mark Waller make of the bulk analytical techniques deployed, or the conduct and results of the trial?

Sir Mark Waller did not express any concerns as to the necessity and proportionality of the holding and use of this dataset.

Please see the response to request 56.

71. Paragraph 95: Please state what steps the Inspectors took. Did the Inspectors audit the use of the BPD? What questions did they ask? Did the Inspectors examine a sample of the queries made, or consider whether they were proportionate and necessary?

The Inspectors assumed an identical role to that usually adopted by the Commissioner, as to which please see the response to request 56.

72. Paragraph 95: Prior to May 2015, had the Inspectors ever previously been involved in the inspection of BPD?

No. Previous inspections had been carried out by the Commissioner and the Head of IOCCO. On this occasion it was carried out by the Head of IOCCO and the Inspectors.

73. Request relating to Paragraph 98.

Paragraph 98 has now been amended: see GCHQ's revised statement dated 15 June 2016.

74. Paragraph 101: How many queries had been run against the database during the period when unauthorised? What use was made of the database whilst unauthorised?

The premise of the question, i.e. that the database was "unauthorised", is mistaken. The non-compliance was that the BPD was not initially recognised as such. No data is available in relation to the number of nature of queries made against the data before it was recognised as BPD and brought within the appropriate regime.

75. Paragraph 115: Please explain the nature and scope of each of the section 94 directions. In particular, did the directions include UK telephone calls, information and about location of individuals?

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Copies of all section 94 directions, together with submissions and associated correspondence, have been provided to the Tribunal.

76. Paragraph 119: Please explain the nature and scope of the expanded directions.

The Respondents cannot respond to this request in OPEN without causing damage to national security.

Copies of all section 94 directions, together with submissions and associated correspondence, have been provided to Counsel to the Tribunal.

77. Paragraph 120: Please state the nature and type of Internet Communications Data obtained. Does the data include communications data of UK persons? What limits are placed on the use of the data? May the data lawfully be used for purposes not related to "UK cyber defence operations"? Has the data been so used? When (if ever) did the Commissioners first carry out an audit of this use of section 94? Please provide the relevant documents and set out the results of the audit.

In respect of the final two questions, please see the response to request 79 in the Response of 20 June 2016. The Respondents are otherwise unable to respond to this request in OPEN without causing damage to national security.

The Internet Communications dataset consists of internet network management data and logs. This includes communications data of UK persons. Use of the data is subject to the usual GCHQ safeguards. The data can be, and has been, used lawfully for purposes not related to UK cyber defence operations.

78. Paragraphs 133-151: Please disclose the records of the meetings, the documents discussed at the meetings and any correspondence prior to and after the meeting.

These meetings are not formally minuted by GCHQ. GCHQ keeps a file note for internal purposes, and there is an agreed list of actions. These cannot be disclosed in OPEN without damaging National Security. The documents discussed were the s.94 Directions themselves, the applications to the Secretary of State for those Directions, and the correspondence with the organisations on whom the Directions were served. These cannot be disclosed in OPEN without damaging National Security. Correspondence after the meetings covers progress against any actions agreed during the inspection. This cannot be disclosed in OPEN without damaging National Security.

Copies of these documents have been provided to the Tribunal and redacted OPEN versions of relevant file notes will be served.

79. Generally on BCD: Please state the precise scope and extent of oversight provided by the Interception of Communications Commissioner, including disclosure of the actual terms of the agreed non-statutory scrutiny of Sir Swinton Thomas. Is Sir Anthony May's July 2015 report correct that such oversight was limited to only certain aspects of safeguards? What were the express terms on which the Intelligence Services Commissioner provided oversight? Please disclose all of the relevant documents.

Prior to the Prime Minister's request to Sir Anthony May in 2015, section 94 oversight had been conducted:

(i) At GCHQ, by IOCCO (Sir Swinton Thomas) between 2004 and 2006, and by the Intelligence Services Commissioner (Sir Peter Gibson, and subsequently Sir Mark Waller) between 2006 and 2015; and

(ii) At MI5, by IOCCO (Sir Paul Kennedy, and subsequently Sir Anthony May) from 2007 to 2015.

The reference at paragraph 4.7 of Sir Anthony May's July 2015 Report is to IOCCO's oversight of section 94 material held at MI5.

With regard to the position at GCHQ from 2004 to 2015, the Commissioner's oversight was not provided on express, agreed, terms. However, as a matter of practice, in advance of each inspection visit the Commissioner was provided with a list setting out details of all the extant s.94 Directions and any that had been cancelled since the previous inspection (these lists cannot be disclosed without damaging National Security). On the basis of the list the Commissioner selected one or more Directions. During the visit the Commissioner examined the relevant Direction or Directions, the applications to the Secretary of State for those Directions (which included the necessity and proportionality justifications), and the correspondence with the organisations on whom the Directions were served. As noted above, these cannot be disclosed without damaging National Security. Sessions were scheduled to give him the opportunity to question those members of GCHQ involved in applying for the relevant Direction or Directions, those responsible for putting them into effect, and analysts who made use of the data obtained under them. The Commissioner was also provided with information on the extent to which s.94 data contributed to intelligence reporting.

The position in respect of the Security Service is addressed in response to request 88 below.

80. Paragraphs 133-135, 137: Please state what steps Sir Swinton Thomas and Sir Peter Gibson carried out by way of non-statutory scrutiny of section 94 directions. In particular, was any audit ever carried out of the granting of section 94 directions or the use (in particular proportionality) of section 94? Did the 'review' simply consist of reading a briefing and receiving a presentation?

See the responses to requests 78 and 79 above.

81. Paragraph 139: Was Sir Mark Waller informed about the MILKWHITE programme, under which section 94 data is made available outside the security and intelligence agencies? What audit did Sir Mark Waller carry out of the use of section 94 data?

The existence of "the MILKWHITE programme" is neither confirmed nor denied.

In respect of audits of the use of section 94 data:

(i) **Bulk communications data obtained by means of a section 94 direction is and was held alongside communications data obtained by means of interception under a section 8(4) warrant.**

(ii) **As the combined data includes communications data obtained by means of interception under a section 8(4) warrant, use of the combined data would have fallen to be overseen by the Interception of Communications Commissioner.**

(iii) **For the avoidance of doubt, the Interception of Communications Commissioner would not know, without additional work, whether it had been obtained by means of a section 8(4) warrant or pursuant to a section 94 direction.**

(iv) **In addition, the Intelligence Services Commissioner also considered the safeguards put in place to identify and address potential abuse of GCHQ's systems. Those systems included, but were not restricted to, those holding section 94 data.**

82. Paragraph 140: Please disclose the records of this meeting in full. The gist is inadequate, in particular as Sir Mark Waller does not appear to have carried out any audit of use, and there does not appear to have been certainty as to whether he had authority to do so.

See the responses to requests 78 and 81 above.

83. Paragraph 141: Did Sir Mark Waller carry out any audit of the use of section 94 data?

See the responses to requests 78 and 81 above.

84. Paragraph 142: Did the Secretary of State approve the request for continued use of the section 94 directions after the end of the pilot? Please disclose the relevant documents. Did Sir Mark Waller audit the use of the material obtained? What did his review consist of? What documents were made available to him?

The Secretary of State did approve the request for continued use of the section 94 Directions after the end of the pilot. The relevant documents cannot be disclosed in OPEN without damaging National Security.

In respect of audits of use, see the response to request 81 above.

Sir Mark Waller did review the use of the dataset(s) in question at the inspection visit. His review consisted of an initial check that the documentation (BPDAR) was in order, gave a good case for acquisition and retention of the dataset(s) including necessity, proportionality and risk of collateral intrusion. He discussed the operational work of the dataset(s) with those who own the dataset(s), asking questions particularly around the issues of necessity, proportionality and collateral intrusion. Thus he looked at the overall use and purpose of the data rather than the specific requests made of the data.

Copies of these documents have been provided to the Tribunal and redacted OPEN versions of relevant file notes will be served.

85. Paragraph 144: What is the basis of saying that "Sir Mark Waller appeared reassured"? Please explain the statement about acquiring private information. All information obtained under section 94 is private. Was Sir Mark Waller's attention drawn to Articles 5 and 6 of the e-Privacy Directive? Please disclose the minutes of the meeting.

During the December 2012 inspection Sir Mark Waller's request for further clarifying information and his subsequent comments indicated that he was reassured. During the June 2013 inspection Sir Mark Waller requested that future submissions seeking section 94 Directions show due consideration into the level of intrusion into privacy, risk of collateral intrusion and associated proportionality considerations and safeguards. Articles 5 and 6 of the e-Privacy Directive were not discussed during the inspection.

See also the response to request 78 above.

86. Paragraphs 145, 146, 147 and 148: Did Sir Mark Waller carry out any audit of the use of section 94 data? What did his review consist of in each case?

See the responses to requests 79 and 81 above.

87. Paragraphs 150-151: Please state what steps the Inspectors took on each occasion. Did the Inspectors audit the use of the BCD obtained under section 94? Did the Inspectors examine a sample of the queries made, or examine whether they were proportionate and necessary?

The inspection visits by staff from the Interception of Communications Commissioner's Office were conducted exactly as if the Commissioner had been present, although GCHQ provided fewer additional briefings outside the formal inspection sessions.

Security Service Witness Statement

88. Paragraph 136: Please state what steps the Commissioners took on each occasion a

review was carried out. Did the Commissioners audit the use of the BCD obtained under section 94? Did the Commissioners example [*sic.* ; presumably "examine"] a sample of the queries made, or examine whether they were proportionate and necessary?

Oversight by Sir Paul Kennedy

The Commissioner reviewed samples of requests for authorisation (for access to the database) and the related authorisations. He did not carry out any additional audit of the use of the CD obtained.

The practice, in relation to his inspections, was that the Commissioner would (prior to his inspection) select the requests/authorisations that he wished to review and MI5 would then provide to the Commissioner the paperwork for those requests/authorisations. That paperwork would describe, in particular, the necessity and proportionality of the proposed request of the database. At his inspection the Commissioner would then review those requests/authorisations he had selected.

MI5 confirm that requests/authorisations were reviewed by the Commissioner at each of his 6 monthly reviews over the period from June 2007 until October 2012 (Sir Paul Kennedy's last inspection as Interception of Communications Commissioner).

The inspections of the database would take place at the same time as the Commissioner was inspecting interception warrants.

Oversight by Sir Anthony May

Sir Anthony May (in his role as Interception of Communications Commissioner) received an initial briefing in relation to the database at his first interception inspection undertaken in May 2013. At this inspection the Commissioner also reviewed requests / authorisations that he had, previously, selected.

In February 2014, Sir Anthony May received a detailed briefing in relation to the database and carried out an inspection of requests / authorisations of the database. Sir Anthony May determined that future oversight of the database should be carried out during the annual communications data inspections undertaken by IOCCO inspectors.

Oversight following the appointment of Sir Stanley Burnton

In December 2015, IOCCO inspectors were provided with full access to the MI5 electronic system that processes authorisations for access to the database (and communications data requests made to CSPs) and they undertook query based searches and random sampling of

the MI5 system for authorising access to the database and reviewed requests / authorisations relating to the database.

89. Paragraphs 137-139: Please provide a copy of the briefings referred to and the further explanation given to Sir Stanley Burnton.

The briefings referred to were provided orally. The Security Service is, accordingly, unable to provide of copy of them.

90. Paragraph 145: Please identify the proportion of cases involved. In each case, please identify whether the DP was independent from the investigation.

The total number of these instances of non-compliance, over the period from 1 November 2010 to date, equates to less than 0.1% of the number of requests of the database.

In relation to these instances of non-compliance:

(a) **Approximately 95% of these non-compliant requests were authorised by DPs who were independent of the investigation concerned. These requests were made by analysts, not the desk officers conducting the investigations, and the DPs who authorised these requests were line managers in the analysts' team and thus not part of the investigative team.**

(b) **The remaining 5% of these non-compliant requests were emergency/out of hours authorisations, provided by DPs who were part of the investigative team.**

91. Paragraph 146: Please identify the proportion of cases referred to whether [*sic*] the justification was written up retrospectively and the proportion of cases where it was not written up at all.

The best particulars that the Security Service is currently able to give in OPEN are that in relation to 8% of these non-compliant requests there was never any written justification.

<u>210 non-compliant requests were discovered. Of those:</u>

(a) **<u>174 were authorised without a written justification in place at the time of the authorisation;</u>**

(b) **<u>in 16 cases there was no write up (hence the figure of 8% previously provided); and</u>**

(c) **<u>in the remaining 20 cases the error was that the application process was not properly completed. This error also occurred in 8 of the requests referred to at (a) above.</u>**

92. Paragraph 147: Please disclose the documents evidencing the reporting of the error and a copy of the "reminder".

The Respondents cannot respond to this request in OPEN without causing damage to national security.

These documents have been provided to the Tribunal.

93. Paragraph 147: How many staff made the errors described? Has any disciplinary action been taken against the staff responsible for the error?

88 staff (63 analysts and 25 DPs) were involved in these instances of non-compliance.

Questions of disciplinary action are under ongoing consideration.

SIS Witness Statement

94. Paragraph 57: Please disclose a copy of the Cabinet Office report.

This request is still under consideration. The Respondents aim to be able to respond to it on or before the hearing on 7 July 2016.

This document has been disclosed to the Tribunal. A redacted OPEN version will be provided.

95. Paragraph 61: What bulk personal data was searched and on how many occasions? When did the improper conduct occur? What was the suspected purpose of the improper searches? How was the misuse detected?

The Respondents cannot respond to the questions regarding what bulk personal data was searched and on how many occasions in OPEN without causing damage to national security.

The searches were carried out on the database, which holds all of SIS's BPDs. Details as to the number of such searches are given in paragraph 61.

All three instances were discovered by the SIS audit team.

In relation to the rest of the request, it is not accepted that anything further falls for disclosure other than that which has already been disclosed.

Exhibits to witness statements

96. MI5 p.815/13 Please identify the aspects of "data management and oversight" which "remain weak and require enhanced oversight". Please explain the period in which such management or oversight was weak.

This request is still under consideration. The Respondents aim to be able to respond to it on or before the hearing on 7 July 2016.

The document in question dates from late 2014 and makes references to aspects of "data management and oversight" which "remain weak and require enhanced oversight."

By data management and oversight being considered "weak", it was meant that improvement would be required in future because, at that time, MI5 recognised that it faced a number of issues in relation to the growing volumes of data it was managing (all types of data, not just BPD), and that aspects of its data management, authorisations, and governance required a refresh.

It is important to note that the reference to "weaknesses in ... oversight" in this document related to internal governance, rather than external oversight. Some of the processes in relation to the management of data had changed because of reprioritisation and changes in staff. In addition, it was recognised that MI5 would need to evolve its existing data governance arrangements to meet its aspirations for future tri-agency collaboration.

Specifically, the aspects of data management and oversight to which this related were:

i. Sharing and moving internally

   It was unclear what the process was for making the decision to move data. The compliance team were having difficulty implementing new more onerous processes in the business because of the problem of resourcing this alongside business as usual.

ii. External data sharing

iii. Data deletions (i.e. the need to enhance decision making and [REDACTION])

Since then, improvements have been made in relation to all three issues.

97. MI5 p. 819 Please disclose the draft and final letters to the Commissioners and any responses.

This request is still under consideration. The Respondents aim to be able to respond to it on or before the hearing on 7 July 2016.

A redacted version of the letter to the Commissioner will be disclosed. It is not believed that there was any response to the letter.

Other

98. Please disclose copies of the 2010 Review of Agency Handling of Bulk Personal Data and the Hannigan Review (if different from the Cabinet Office review of the same year).

This is the document requested at request 94.

29 June 2016
Amended on 14 July 2016

JAMES EADIE QC
ANDREW O'CONNOR QC
RICHARD O'BRIEN