Amendments are double-underlined

Witness: GCHQ Witness
Party: 3rd Respondent
Number: 1
Exhibit: GCHQ1
Date: 8.7.16

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

AMENDED WITNESS STATEMENT OF THE GCHQ WITNESS

I, the GCHQ Witness, Deputy Director in the Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1. I am Deputy Director Mission Policy at GCHQ. In that role, I am responsible for drawing up the operational policies that underpin GCHQ's intelligence gathering activities and for ensuring that they are complied with. I have been in this role since 5 January 2015, having previously served as Deputy to my predecessor. I have worked for GCHQ in a variety of roles since 1997.

2. I am authorised to make this witness statement on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based

upon documentation made available to me and from discussions with others within the department.

3. Attached to this statement and marked Exhibit 'GCHQ1', are 14 relevant documents. Page numbers below are references to Exhibit 'GCHQ1'.

4. In this statement I use the term "the Intelligence Services" to refer, collectively, to the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. I also use the terms "MI5", "SIS" and "GCHQ" to refer to those bodies individually.

5. In this statement I will address:

   a) GCHQ's use of Bulk Personal Datasets and its importance and value in fulfilling GCHQ's statutory functions;

   b) The relevant safeguards and oversight mechanisms for BPD;

   c) GCHQ's use of directions made pursuant to section 94 of the Telecommunications Act 1984 and its importance and value in fulfilling GCHQ's statutory functions; and

   d) The relevant safeguards and oversight mechanisms for bulk communications data (BCD) acquired by section 94 of the Telecommunications Act 1984.

6. I adopt the evidence of the MI5 Witness in respect of the current threat picture and of the challenges faced by the SIA in terms of the current threat.

A. GCHQ'S USE OF BULK PERSONAL DATASETS

7. GCHQ's use of BPD has its origins in the need to obtain information from datasets held by liaison partners and other UK Government and private sector bodies which provided context for reporting. Historically GCHQ would have interrogated these datasets by referring each query to the bodies that hold them who are regarded as the 'data owners'. The acquisition and in-house exploitation of bulk data by GCHQ has evolved over a number of years, driven by changes to the threat facing the UK and improvements in technology, which have made it possible to extract value from this kind of data.

GCHQ's in-house exploitation of BPD

8. Between 2012 and the Spring of 2016 the principal repository for of GCHQ's BPDs has been a dedicated corporate tool. This tool enables analysts to quickly run searches against datasets using selected Target Detection Indicators (TDIs). A TDI is a piece of metadata

that is unique to a particular user or machine, and persistently associated with only that user or machine. Examples include e-mail addresses, media access control (MAC) addresses, telephone numbers and passport numbers. Analysts can run searches using TDIs against a multitude of datasets, with a view to enriching the seed selector and giving it more context.

9. The datasets which sit behind the tool are linked together by field types. This enables very powerful, and very fast, data fusion. For example, a mobile number is queried; it hits in a dataset which provides you with a name and address, but also returns a National Identity Card number (NIC). The tool automatically searches the NIC against all the other datasets. It hits on the NIC in some more datasets and returns five new telephone numbers, plus a passport number.

10. Any queries run on the tool require the analyst to make a Necessity and Proportionality Statement in which they must specify the relevant purpose of the query (National Security, Economic Well-being, or in support of the prevention or detection of serious crime), the specific intelligence requirement that the activity seeks to meet, and a free text justification of the search.

11. During the Spring of 2016 BPDs held on this tool were transferred to a new corporate tool. This has the same functionality as the tool it replaced.

BPDs not held in the main corporate tool

12. Since 2014 a number of GCHQ's travel-related Bulk Personal Datasets have been held on a new travel data tool that uses various different feeds of information to build a picture of the travel of individuals. Data in this tool is also accessible by analysts in the other two Agencies.

13. In addition there are a number of active BPDs held outside of the above two tools. In the majority of cases the reason why these BPDs are held separately is because they are used in combination with datasets which do not contain bulk personal data. It is therefore necessary for them to be held with those non-BPD datasets. In a small number of cases the reason they are separately held is due to the nature of the data e.g. for reasons of exceptional sensitivity, the need for specialised analytic capabilities, or where they are undergoing initial assessment prior to ingestion.

Importance and value of BPD

14. Bulk personal datasets comprise personal data relating to a number of individuals, the majority of whom are unlikely to be of intelligence interest. BPDs can be acquired in various ways. Some are from open source data while others are obtained via other covert means such as interception, Equipment Interference or from human intelligence sources.

The Intelligence Services hold the data electronically and analysts will only look at the data relating to the minority who are of intelligence interest. The Intelligence Services do this by asking specific questions of the data to retrieve information of intelligence value.

15. The analysis of BPD by the Intelligence Services is a critical part of their response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens in a digital age.

16. Exploitation of BPD is an essential tool that is used on a daily basis, in combination with other capabilities, right across the Intelligence Services' operations. It plays an integral role in enabling the Intelligence Services to exercise their statutory functions. Without it, the Intelligence Services would be significantly less effective in protecting the UK against threats such as terrorism, cyber threats or espionage.

17. BPD enables the Intelligence Services to focus their efforts on individuals who threaten our national security or may be of other intelligence interest, by helping to identify such individuals without always having to rely on more intrusive investigative techniques. It helps to establish links between subjects of interest or better understand a subject of interest's behaviour. BPD also assists with the verification of information obtained through other sources (for example agents) during the course of an investigation or intelligence operation.

18. Travel data, for example, helps the Intelligence Services to establish an understanding of the travel history of a subject of interest which, in turn, enables them to disrupt the activities of those who mean us harm. BPD can be used in order to obtain valuable information about pattern of movement which helps to identify previously unknown subjects of interest.

19. Using BPD also enables the Intelligence Services to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations.

20. A list of people who have a passport is a good example of a BPD that the Intelligence Services might hold - it includes personal information about a large number of individuals, the majority of which will relate to people who are not of interest to the Intelligence Services. Other examples of BPD might include population data (such as the electoral register), commercial data, data relating to communications (such as the telephone directory), financial data (such as data relating to suspicious financial activity), and data acquired from other intelligence or law enforcement agencies (such as data about individuals with access to firearms).

21. GCHQ shares BPDs with MI5 and SIS, subject to any such sharing being necessary and proportionate and for one of GCHQ's statutory purposes. Were we to share with foreign partners, that would be on the same basis. All such sharing is documented in the form

used to authorise acquisition and retention of the particular BPD. These forms are discussed below.

22. I note that it is suggested at paragraph 45 of the witness statement of Camilla Graham Wood that *"there is a potential indication of the use of covert means against Other Government Departments"*. For the avoidance of doubt, any such allegation is denied. Any BPDs obtained from Other Government Departments ("OGDs") are obtained with the approval of those OGDs.

The types of BPD in use

23. GCHQ holds BPDs in the following categories: Commercial; Communications; Financial; Identity; and Travel."

24. We hold no BPDs consisting of medical records, whether sourced from the NHS or other health providers; information which relates to a medical condition can however appear in a BPD e.g. travel. Some people may include information regarding medical conditions in booking data or in their passports.

The meaning of sensitive data

25. The phrase "sensitive data" in the context of BPD can have three different meanings depending on context.

26. Section 2 of the DPA defines the sensitive classes of personal data as data which is about:

- Racial or ethnic origin
- Political opinions
- Religious belief or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health union
- Physical or mental health or condition
- Sexual life

27. In addition, GCHQ treats a number of other categories of information as sensitive. These include – but are not limited to - areas such as legal professional privilege, journalistic material and financial data.

28. The handling arrangements applicable to certain data can also characterise the data as 'sensitive' based on other facts such as the nature of the capability or source by which it has been acquired, the level of intrusion of the information itself or the operational requirement that it will support.

The meaning of corporate risk

29. In the context of BPD the phrase "corporate risk" refers to the damage that would potentially be caused to GCHQ operations or reputation by exposure of a dataset. A variety of factors may be relevant here, including the size of the dataset (the number of people whose data is included), the sensitivity or potential vulnerability of the source of the data, and the categories of people whose personal data is included (e.g. where a significant proportion of the data might relate to the UK nationals).

B. SAFEGUARDS AND OVERSIGHT MECHANISMS FOR BPD

Compliance Guide

30. GCHQ's use of BPD, like all areas of GCHQ's operational activity, is, and has throughout the entire period with which this claim is concerned been subject to the safeguards set out in GCHQ's Compliance Guide.

31. I exhibit the relevant version of the GCHQ Compliance Guide for the period June 2005 to 2010 at pages 89 to 146 of Exhibit 'GCHQ1'.

32. I exhibit the relevant version of the GCHQ Compliance Guide for the period 2010 to June 2014, as amended from time to time, at pages 147 to 162 of Exhibit 'GCHQ1'.

33. I exhibit the relevant version of the GCHQ Compliance Guide for the period June 2014 to the present, as amended from time to time, at pages 5 to 24 of Exhibit 'GCHQ1'.

34. The Compliance Guide provided, and continues to provide, overarching safeguards relating to the requirements that all operational activity must be authorised, necessary and proportionate and guidance as to those requirements, as well as specific guidance in relation to specific areas of operational activity. However, in the case of BPD, more specific guidance is, and has been, provided in the following documents.

BPDAR form and guidance for completing the BPDAR form

35. Between October 2012 and January 2016 applications for authorisations to acquire BPD, and to renew or cancel the use of BPD, were made on a Bulk Personal Data Acquisition and Retention form ("the BPDAR form"). I exhibit this form at pages 43 to 50 of Exhibit 'GCHQ1'.

36. Guidance has also existed throughout the same period for completing the BPDAR form ("the BPDAR Guidance"). This guidance, as amended from time to time, is exhibited at pages 163 to 166 of Exhibit 'GCHQ1'.

37. The BPDAR form in use between October 2012 and January 2016 required details of the BPD to be set out, together with the intelligence case, proposed retention period and access controls. In addition details of the *"Extent of potential intrusiveness"* were required to be completed. This required consideration of whether a number of specified data "fields" were contained in the BPD (e.g. name, date of birth, banking/credit cards/other financial information, travel details, medical details, religious information) as well as whether the dataset contained *"a high proportion of data on people of no probable intelligence interest"*. In addition the Data Owner was required to state whether the BPD contained information about minors. The relevant team was then required to provide an assessment of the intrusiveness and sensitivity of the BPD, having consulted with the Data Owner.

38. In light of that assessment, the Authorising Officer could provide authorisation only after a declaration that:

"I am satisfied that the acquisition of this dataset is necessary and proportionate in relation to one or more of GCHQ's authorised purposes and that it will be handled appropriately."

39. When authorising the acquisition and retention of the BPD, the Authorising Officer was also required to state a period after which the retention of the BPD should be reviewed.

40. The BPDAR form also contained, at Section B, sections addressing reviews of the retention of BPD. Both at the first and second reviews, the intelligence case for retention, or reason for cancellation, was required to be set out, together with a declaration, by the Authorising Officer, that he/she was *"satisfied that the use of this dataset continues to be necessary and proportionate."* Again, a period was required to be given after which the retention of the BPD required to be reviewed.

41. The BPDAR Guidance noted that:

"The BPDAR process is an internal policy authorisation used to authorised acquisition and/or retention of operational data by GCHQ, where the data is:

– Bulk in nature (i.e. not narrowly focused on a particular target), and

– Personal (i.e. deals with individuals and contains real names)."

42. It added that:

"The purposes of the BPDAR process are:

– To account for GCHQ's acquisition and retention of bulk personal data, so that we can demonstrate to our oversight bodies that a suitably senior and experienced GCHQ officer has considered whether the acquisition and ongoing retention of the data is necessary and proportionate in relation to one or more of GCHQ's authorised purposes under the Intelligence Services Act, and

– To ensure that we have a better knowledge of what bulk personal data we hold and where it is stored."

43. Responsibility for the BPD was specifically stated in the BPDAR Guidance to lie with a "Data Sponsor" and a "Data Owner" (as referred to in the BPDAR form). The BPDAR Guidance explained what Section A of the BPDAR form should contain. This included:

"Intelligence case

The Data Sponsor must provide a statement of the intelligence case for acquiring the data, including why he believes it to be necessary and proportionate to hold bulk personal data of this nature and scale, and what he expects the likely intelligence benefits will be."

44. In relation to "Section A: Extent of potential intrusiveness" the BPDAR Guidance noted that:

"The Authorising Officer must be a named individual on the Approvals list for BPDARs…He is responsible for considering the business case in light of the intrusiveness and sensitivity of the data, and deciding whether the acquisition of the data meets the criteria of necessity and proportionality..."

45. In relation to renewals/cancellations of BPD the BPDAR Guidance stated that:

"The Data Sponsor must provide a statement of the value of the data to date (including what intelligence benefit has resulted from exploitation of the data) and why the continued retention of the data is believed to be necessary and proportionate. Is the data unique? Could the intelligence benefit be obtained by other means? If access to the data were lost, how difficult would it be to re-establish it?"

46. Any reason for deletion of the data also had to be stated.

47. The BPDAR Guidance also referred to the role of the Retention Review Panel:

"Section B: Outcome of Review Panel

A 6-monthly Retention Review Panel will be held (currently September and March) to ensure that all retention (and, where relevant, continued acquisition) of bulk personal data remains necessary and proportionate. The Review Panel will consider the cases submitted by Data Sponsors and will decide whether datasets should continue to be retained (and acquired). The Review Panel will also specify the next retention review date for each dataset – this may be for 12 months (typically) or 6 months (for especially sensitive data, or where the data's value is still unproven."

48. The BPDAR Guidance specifically noted that the Retention Review Panel could make comments or requests for information on the appropriate section of the BPDAR form ("Section B: Review Panel comments or requests for additional information").

49. The BPDAR form referred to above was replaced in January 2016. The BPDAR form in use since then is exhibited at pages 25 to 42 of Exhibit 'GCHQ1'.

50. The current BPDAR form is completed by a "Requester" for consideration by an "Endorser" and authorisation by an "Authoriser" (the terms used at Section 6 of the GCHQ BPD Handling Arrangements, which I exhibit at pages 71 to 80 of Exhibit 'GCHQ1'). The new BPDAR form is in many respects similar to its predecessor, but also requires, amongst other things:

    a) More detailed consideration of the proportion of the BPD which related to *"people of no probable intelligence interest"* and *"children/minors"*. The BPDAR form requires consideration of whether that proportion was *"High, Medium, Low, Zero, Not Known"*;

    b) Consideration of whether any of the data in the BPD would be removed before the BPD was provided to analysts. This would be appropriate, for instance, if particularly sensitive data were to be removed from the BPD before exploitation;

    c) Endorsement by a legal adviser;

    d) Consideration of whether the BPD is *"likely to include confidential comms (e.g. Legal Professional Privilege (LPP), journalistic sources or spiritual/religious counselling)"*;

    e) Details to be given of the *"plans for exploitation"* of the BPD;

    f) An assessment to be made by the Authoriser of the intrusiveness and sensitivity of the BPD (assessed as "High", "Medium" or "Low");

    g) A selection of a period of six, 12 or 24 months after acquisition when the justification for the continued retention of the BPD is to be reconsidered; and

    h) Completion of sections, as appropriate, concerning experimental use of the BPD, disclosure of the BPD to an external organisation, or the BPD's continued retention (following a review).

Data Sharing Requests

51. Requests by other security and intelligence agencies to share GCHQ's BPDs must also be made on a specific form, which was first used in June 2014, and amended in October 2014 (exhibited at pages 59 to 64 of Exhibit 'GCHQ1') ("the Data Sharing Request"). The Data Sharing Request, which is used by all the security and intelligence agencies, requires, amongst other things, the business case and justification (including necessity and proportionality) for the request for BPD, together with a statement of the intended use and dissemination of the BPD and the proposed data retention period. The Data Sharing Request must also be completed by the "donor" agency, which must give details, amongst other things, of the "intrusion of the dataset".

BPD Review Panel

52. GCHQ has had a BPD Review Panel since 2010. From 25 March 2015 its terms of reference were as set out at pages 59 to 64 of Exhibit 'GCHQ1'. This notes that the purpose of the BPD Review Panel is:

"to provide effective senior oversight of the lifecycle of Bulk Personal Data in GCHQ's possession, thereby providing assurance that GCHQ handles Bulk Personal Data appropriately and in accordance with the law."

53. The BPD Review Panel has to be chaired by a Director or Deputy Director of GCHQ. Its primary functions are:

" - to consider requests from the business to authorise continued retention and exploitation of Bulk Personal Datasets, with particular regard to necessity and proportionality, and
- to satisfy itself that GCHQ's handling of Bulk Personal Data throughout its life-cycle meets required standards, as described in the SIA Bulk Personal Data Policy."

54. The reference to the SIA Bulk Personal Data Policy is to the policy agreed by the security and intelligence agencies in February 2015. This has been exhibited by the MI5 Witness at pages 309 to 318 of Exhibit 'MI51'.

55. The BPD Review Panel's process is set out in its terms of reference as follows:

"The Panel will meet approximately every six months, typically in March and September.
It will review paperwork relating to datasets that fall due for review at each meeting, considering especially:
- the adequacy of the information provided in the Bulk Personal Data form,
- the quality of the case (if any) made by the business for the retention of the Bulk Personal Dataset, in terms of its value and level of use set against the sensitivity, intrusiveness and corporate risk of continued retention, and

– the arrangements and plans for the continued acquisition (if applicable), storage, exploitation, sharing and ultimate deletion/destruction of the data.
If a request for retention is submitted, the Panel will either:
– authorise retention for whatever period it sees fit, [redacted], or
– authorise provisional or temporary retention with stipulations or conditions, or
– reject the request and require the deletion/destruction of the Bulk Personal Dataset in question.
If no such request is received, the Panel will require evidence of the deletion of the Bulk Personal Dataset.
At each meeting, the Panel will also:
– require evidence of the satisfactory completion of actions from the previous meeting, especially deletion of Bulk Personal Datasets where permission to retain was refused; and
– confirm or modify its assessment of the intrusiveness and sensitivity of GCHQ's possession of the datasets under review.
All Panel decisions must be recorded."

GCHQ BPD Handling Arrangements

56. On 4 November 2015 the GCHQ BPD Handling Arrangements, made under section 4(2)(a) of the Intelligence Services Act 1994, came into force. A copy of the GCHQ BPD Handling Arrangements is exhibited at pages 71 to 80 of exhibit "GCHQ1". These set out detailed provisions (which are not repeated here) in relation to various stages of the lifecycle of a BPD, namely:
    a) Acquisition;
    b) Use;
    c) Disclosure;
    d) Retention;
    e) Deletion/Destruction.

Statutory Codes of Practice

57. Depending on the means of acquisition of the BPD, one of the Codes of Practice issued under the Regulation of Investigatory Powers Act 2000 ("RIPA") or Intelligence Services Act 1994 ("ISA") may be relevant and applicable.

58. GCHQ's current Handling Arrangements (paragraph 2.6) recognise that in the event that, for example, RIPA or ISA statutory powers are used to acquire a BPD (for instance by equipment interference or interception) then the applicable regime relating to those powers (including any applicable RIPA or ISA Code of Practice) will need to be complied with, and the requirements of the BPD Handling Arrangements will apply in addition to and/or in parallel with that statutory regime. Accordingly, if GCHQ wished to seek to obtain a BPD through equipment interference, we would seek the necessary equipment interference warrant from the Secretary of State and, in parallel with that, would follow GCHQ's internal process for the acquisition of BPD.

Secure systems and Security Operating Procedure

59. All GCHQ corporate systems are accredited to hold data with a classification of TOP SECRET - STRAP. The accreditation involves checking that the system has a sufficiently high degree of security to prevent access by unauthorised individuals. In addition, access to data is controlled by confining such access to defined groups of users. Furthermore, users are required to read the specific security policies relating to the use of particular systems and capabilities. I exhibit an example of such a policy, GCHQ's Removable Media Policy, at pages 167 to 174 of exhibit "GCHQ1".

Audit

60. I have already referred in paragraph 10 above to the fact that any queries run on the tool require the analyst to make a Necessity and Proportionality Statement. These statements are subject to audit. The standard against which the free text justifications are tested is that somebody not directly involved in the operational activity can satisfy themselves that the query was necessary and proportionate in the circumstances. In practice it is usually the Legal and Policy Lead (LPL) for each area that does the audit for their area. These individuals will generally be of the same grade as the person who ran the queries, and in the same area in order that they can understand how the justification for running the query matches with the stated intelligence requirement.

TRAINING ON BPD USE WITHIN GCHQ

61. GCHQ provides extensive training in the use of the main corporate BPD tool and the new travel data tool. All staff, integrees from other Agencies and Departments and contractors working at GCHQ are required to undertake a Mandatory Legalities Overview (MLO) on-line training package and to pass the associated test. The MLO contains a section addressing GCHQ's holding of bulk personal data. The relevant text is as follows:

"Bulk Personal Data

GCHQ holds some large datasets which contain the names of individuals in a number of countries which it exploits for intelligence purposes.

Examples include travel data, mobile phone subscriber lists and entry visa applications. Many of these datasets have been provided by other agencies."

Given that these datasets include many individuals who are never likely to be intelligence targets, the holding of such datasets is especially sensitive.

GCHQ therefore takes special measures to ensure that we can account for this data and justify our use of it.

We have a formal policy requiring each bulk personal dataset to have a sponsor at GC8 or above, to ensure that:

- *GCHQ has a full record of the dataset (what, where, why);*
- *we understand the intelligence value we get from it;*
- *it is deleted when our possession of it can no longer be justified.*

Remember this: GCHQ has special procedures in place to account for bulk personal data."

62. The MLO must be retaken every two years.

63. Staff whose roles involve access to operational data are required to take Advanced Mission Legalities (AML) training, and again, to pass the associated test. This on-line course contains the following text relating to BPDs:

"Bulk Personal Datasets (BPD)

These are large sets of data containing information about identifiable individuals, most of whom are of no intelligence interest. (The full definition can be found in the Joint SIA BPD Policy.)

GCHQ's possession and use of such datasets in support of its intelligence activities is lawful and legitimate but nonetheless particularly sensitive. Our acquisition, use, disclosure and ongoing retention of these datasets must therefore be authorised by a senior member of staff, currently Deputy Director Mission Policy or Director Risk & Compliance.

As of August 2015, a comprehensive updated authorisation process is in development. Until it is ready, please contact the compliance Team if you need further details."

64. AML must also be retaken every two years. The *"comprehensive updated authorisation process"* came into effect on 15 November; the training package will be updated to reflect this at the next opportunity.

65. In addition to the legalities training GCHQ provides extensive training in the use of the main corporate BPD tool, through an on-line e-learning package. This is an hour-long module which provides an introduction to using the tool to query across a multitude of collateral datasets, helping to enrich selectors with context and identify new selectors for targets. It also provides the legal and policy information required to handle the data appropriately. The course is a pre-requisite for anyone who wants an account on the tool. Also to get an account AML training must also be completed and a business case provided to IT Services. There is also a hard copy Learning Guide. As with the main GCHQ BPD tool, a range of training materials are available to users for the new travel data tool. This includes a 10-minute Travel Data Policy Training module designed to give a basic introduction to the types of Travel Data available to GCHQ analysts and the legal and policy information required to handle the data appropriately. It is a pre-requisite for anyone who wants an account on the travel data tool. Also to get an account AML training must also be completed and a business case provided to IT Services. The Mission

Policy team has established a dedicated on-line "group" covering BPDs on GCHQ's internal collaborative tool. The group pages are owned and updated by the compliance team within Mission Policy. They contain links to the BPD form and guidance, the GCHQ BPD closed handling arrangements and BPD draft code of practice. There is an option for staff to ask questions relating to BPDs. The text of the "overview" section reads as follows:

"This group has been set up as a knowledge share for matters relating to GCHQ's acquisition and retention of 'Bulk Personal Data' (BPD). The recently introduced (Nov 15) GCHQ Closed Handling Instructions provide guidance on the requirements and scope of the BPD process, particularly in respect of those individuals that hold and manage a BPD. This page will aim to increase awareness of the BPD process, address any frequently asked questions, and act as a helpful point of reference."

66. The group currently has around 90 members, including many of the Legal and Policy Leads who act as points of contact between the Mission Policy team and the operational and technical teams across GCHQ.

INDEPENDENT OVERSIGHT

December 2010

67. Following a review of Bulk Data Holdings by the Security Advisor to the PM (a redacted version of which will be exhibited to this statement), the Intelligence Services Commissioner was invited to oversee the Agencies' BPDs. The initial inspection took place on 6 December 2010 and was conducted by Sir Peter Gibson. He was accompanied by his successor, Sir Mark Waller, for whom this was his first visit to GCHQ.

68. The initial part of the day focused on the context for the inspection, and the legal principles underpinning GCHQ's acquisition of non-targeted bulk personal data. We noted that use of such data was a niche part of GCHQ's business and untypical of the majority of GCHQ's foreign intelligence activity. However, data analysis was a core function of GCHQ (unlike its sister agencies where the function might be concentrated in a specialist area away from the core investigative functions), and GCHQ was consciously moving towards access to non-targeted bulk personal datasets by a wider group of analysts, making such data available as part of the regular fused analysis toolkit. Nevertheless, we noted that GCHQ did not wish to retain large quantities of non-targeted bulk personal data: this would be undesirable on grounds of proportionality and cost.

69. We took Sir Peter and Sir Mark through GCHQ's new formal review process. Sir Peter and Sir Mark were interested in how GCHQ reviewed the retention of its bulk personal data (we explained that we made use of a retention review panel, which meets every six months and is chaired by Deputy Director Operations Policy (now Deputy Director Mission Policy); this review panel orders the deletion of a dataset where it is no longer needed).

70. We took the opportunity to brief Sir Peter and Sir Mark on audit practices for operational data. GCHQ's operational systems (including repositories holding communications data) already oblige those interrogating the data to enter an authorised purpose, a JIC requirement and a short free-text justification. Although we had a well-established procedure to sample and audit these records, bulk personal datasets were not yet routinely included, and in any case the sampling methodology was not well-suited to detecting anomalies in use of such data. We had therefore asked the IT Services Accounting and Audit team to help us monitor any indications of misuse of non-targeted bulk personal datasets. Sir Peter and Sir Mark were very interested in a presentation giving some illustrated examples of the processes and techniques being developed. Sir Peter was satisfied with the rigour of these processes; he also found it interesting to note our routine procedure of requiring analysts to record a justification before acquiring any access to operational bulk data.

71. Sir Peter had selected four datasets from the initial list we had offered, and he was interested to question the analysts involved in use of these datasets in order to establish their value.

March 2011

72. Sir Mark Waller visited GCHQ on 1 March 2011 for a familiarisation visit. While there was a session during which Sir Mark was able to discuss and finalise his selection of BPDs and s.94 Directions ahead of his first formal inspection there was no substantive discussion of BPDs.

73. The formal inspection took place on 29 March 2011. Sir Mark had requested to inspect a number of specific non-targeted bulk personal datasets. He was satisfied that the datasets were necessary. He asked some specific questions with regard to storage of the data. In particular, he asked whether we could take datasets out of the corporate BPD tool once they are in it, and we confirmed that we could. He also asked how we know whether data had been useful. Our response was that analysts are required to fill in a "Technical Data Sheet (TDS) screen when drafting reports. The TDS captured the source(s) of the data that the report was derived from, allowing us to generate data on what sources of data were productive. We mentioned that GCHQ's review panel had approved two financial datasets on the basis that they should be re-reviewed after one month and deleted if not proved to be useful.

74. Sir Mark noted that it would be extremely useful to inform his future report if GCHQ could provide (a) a summary of how GCHQ makes use of, manages and reviews non-targeted bulk personal data, and (b) how we audit usage and what safeguards are in place to ensure proportionate and managed access.

October 2011

75. Sir Mark conducted an inspection on 17-18 October 2011. He examined a specific dataset. The fact that it had led to 26 intelligence reports over the last year (although it was an ageing dataset) left him in no doubt as to its value. He asked whether we deleted datasets that the review panel did not judge worthy of retention, and we confirmed that we did. Sir Mark was pleased to hear that most of GCHQ's operational data is subject to a default data retention period. Sir Mark also examined a second dataset: he was left in no doubt of the intelligence requirements relating to the relevant location, but asked why there was no data in relation to British nationals. We confirmed that this was because the original source of the information did not hold that data. Sir Mark was again interested to know how we monitored potential misuse, though he noted that the risk of misuse was lower for a dataset that did not contain data relating to British nationals.

December 2011

76. Sir Paul Kennedy conducted an inspection on 13 December 2011. We provided some context to the role that Sir Paul had kindly agreed to fulfil on Non-Targeted Bulk Personal Data. The Intelligence Services Commissioner had assumed a non-statutory role in overseeing nearly all the relevant datasets, but for the few GCHQ datasets that were obtained under RIPA authorisation, Sir Paul had agreed to examine them. We also explained the role of the GCHQ Retention Review Panel. On this occasion Sir Paul had chosen to examine a specific dataset and he scrutinised the form completed by the panel after their review of this dataset. He was content that a justification had been properly made out for the retention of the dataset.

March 2012

77. Sir Mark Waller conducted an inspection on 19-20 March 2012. He was satisfied that the acquisition and retention of the three bulk personal datasets he had selected was both necessary and proportionate.

April 2012

78. Sir Paul Kennedy conducted an inspection on 17 April 2012. The Commissioner inspected paperwork associated with a non-targeted bulk personal dataset acquired under the authority of an interception warrant. The Commissioner noted that the dataset potentially had an application to Serious Crime as well as to Counter-Terrorism. We

clarified how users of the corporate BPD tool can use the system's query tool to run queries across multiple datasets and that results would only be obtained in the event of a match. He commented that holding data at all had implications for Human Rights, but this issue was not acute until the point of query. The Commissioner also checked that the retention period could be justified and was satisfied to hear that this type of data was relatively stable and could continue to be useful for such a period. He noted that GCHQ, given its mission, did not hold much data in respect of UK citizens.

October 2012

79. Sir Paul Kennedy conducted an inspection on 3 October 2012. The Commissioner was invited to inspect GCHQ's holding of a highly sensitive and closely held dataset, as part of his non-statutory role in overseeing bulk personal datasets acquired under RIPA authorisation. My predecessor as Deputy Director Mission Policy explained how the acquisition and retention of bulk personal datasets is internally reviewed by a panel of policy seniors. The dataset was relatively new and had yet to be presented to the panel but would be considered at the next meeting of the panel in November. The data was being used for agent spotting/ evaluation and target development and had already proved to be of significant value. The Commissioner commented: "Obviously does help you to evaluate the agent... I can see why it's valuable."

December 2012

80. Sir Mark Waller conducted an inspection on 4-5 December 2012. He considered three BPDs:

    a) In relation to the first dataset, the Commissioner queried what safeguards were in place to prevent analysts from querying against non-targets in an inappropriate way. He was provided with assurances in respect of the need for Necessity and Proportionality Statements for every query. He had spotted that another dataset, of which this dataset was a part, was overdue for review.

    b) In relation to the second dataset, the Commissioner had spotted a discrepancy between the date of the DAA authorising the acquisition of the data and the setting of a 2-month retention period and the date of the data destruction. It was explained in the briefing that this was because there had been significant delays in getting the data into the building and therefore the 2-month retention period had not in fact been exceeded. The Commissioner suggested that it would have been useful to have had this highlighted in the table in the choice letter.

c) In relation to the third dataset, the Commissioner questioned the absence of a DAA form and it was explained that this dataset had arrived in the building before the introduction of the DAA process. However, because the data had not been acquired via a DAA, the requirements to track its progress and report its destruction to Mission Policy were not followed. This had been addressed by the compilation of the form presented to the Commissioner for inspection, which would also form the corporate record of the history of the data in GCHQ. The Commissioner was assured that this should not happen with any datasets that have been subject to the DAA process.

May 2013

81. Sir Anthony May conducted an inspection on 15 May 2013. This was his first formal inspection visit since taking up post as Interception of Communications Commissioner in January 2013, although he had visited GCHQ for familiarisation briefings in January. Sir Anthony examined one BPD derived from Interception. The data that forms the dataset is collected under the authorisation of a warrant. The Commissioner queried how, if the collection takes place outside of the UK, it fits in with his jurisdiction. A senior lawyer provided an explanation.

82. It was explained to the Commissioner that this type of data can be retained, subject to regular review, for longer than the standard data retention period. The reasons for this policy were explained. The Commissioner expressed interest in the storage and retention of bulk personal data and would like to come back to the long retention period for this type of data.

June 2013

83. Sir Mark Waller conducted an inspection on 4-5 June 2013. We briefed him on four BPDs.

a) A travel dataset. All SIA agencies acquire this data but used it for slightly different purposes.

b) A group of financial datasets that GCHQ had acquired from SIS and which also contain biographical information.

c) A separate financial dataset also obtained from SIS, which could be accessed by only two people.

October 2013

84. Sir Anthony May conducted an inspection on 8-9 October 2013. He examined one BPD derived from Interception. Following a discussion of this dataset, Sir Anthony suggested that it might be appropriate to include the small number of non-targeted bulk personal datasets obtained from interception in the listing put forward to Sir Mark Waller for inspection, so that Sir Mark was aware of their existence and nature.

December 2013

85. Sir Mark Waller conducted an inspection on 10-11 December 2013. The Commissioner inspected two datasets. He was satisfied with the business cases for obtaining both sets of data. He noted that there was an outstanding requirement for a strengthened business case for the retention of one of the datasets to be put to the review panel by the end of October. He was assured that, as the business case had not yet been received, the dataset had been quarantined in the corporate BPD tool and would not be made available again to analysts without the approval of the review panel.

86. At the request of Sir Anthony May, Sir Mark had been provided with information relating to the non-targeted bulk personal datasets obtained via interception, so that he was aware of these datasets which come under Sir Anthony's oversight. Sir Mark was asked if he required any further information on these datasets but he indicated that he was happy with what had already been provided.

April 2014

87. Sir Anthony May conducted an inspection on 22-23 April 2014. The Commissioner had been provided with the paperwork on three datasets obtained via interception under RIPA Part I Chapter I. He was given short explanations of the nature and value of these datasets, with which he appeared content.

May 2014

88. Sir Mark Waller conducted an inspection on 28-29 May 2014. The Commissioner looked in more detail at three specific data sets held and challenged GCHQ to justify their retention.

    a) A commercial data set.

    b) A communications data set containing publicly available subscriber data.

    c) A financial data set containing financial data with very strict rules of access.

89. Having reviewed the retention of these three data sets and considered GCHQ's internal review process to assess the acquisition, retention and deletion of data sets the Commissioner was content that GCHQ's holding of personal bulk data sets was both necessary and proportionate.

October 2014

90. Sir Paul Kennedy conducted an inspection on 21-22 October 2014. He examined two BPDs derived from Interception. The Commissioner was provided with a recap of how bulk personal data was handled and overseen within GCHQ. He was taken through the data acquisition and review process. A GCHQ official then provided a briefing on the history of a specific financial dataset. The Commissioner asked how the data was used to meet specific finance related intelligence requirements. The Commissioner expressed no concerns.

91. The Commissioner was briefed on the use of another dataset, which was generated from interception obtained under a warrant, and how it was used to discriminate between targets and non-targets so that non-targets could be excluded from our investigations more promptly and thereby unnecessary intrusion into their privacy could be avoided. As some details are kept on parties not of intelligence interest, the Commissioner was interested in who could access the data. He was reassured when he was told that the file is password protected and only 10 named individuals within a specialist operational team had access. The Commissioner was briefed on the use of another dataset, which was generated from interception obtained under a warrant

November 2014

92. Sir Mark Waller conducted an inspection on 11-12 November 2014. He inspected three datasets.

April 2015

93. Sir Mark Waller conducted an inspection on 21-23 April 2015. He examined two BPDs. It was explained by the operational team that because of the complexity of the data a recently acquired dataset was still being processed and had not yet been ingested into standard GCHQ analytical tools. The tight controls around access to the data were explained and it was anticipated that the data would only ever be accessible to a small number of analysts because of its sensitivity.

94. Another dataset had been acquired for a time-limited trial to investigate what value GCHQ might gain from it. The trial data had only been exposed to approximately 10 analysts; the sample of the available data that had been selected it was deemed likely to contain material relating to GCHQ targets. Obtaining the data in bulk enabled GCHQ to

run bulk analytics against it: the trial had proven the value of the data and an intention to seek approval for sustained access to this type of data was stated.

May 2015

95. Staff from the Interception of Communications Commissioner's Office (IOCCO) conducted an inspection on 6 May 2015. They examined two BPDs derived from Interception.

96. The Inspectors requested a more general briefing at the next inspection visit on the Intelligence Services' trilateral approach to handling of bulk personal datasets. IOCCO stated that they planned to liaise with Sir Mark Waller, who oversees the vast majority of GCHQ's bulk personal datasets, to ensure a common approach between the two Commissioners.

October 2015

97. Sir Mark Waller conducted an inspection on 21-23 October 2015. He examined four BPDs. In one case, having read the paperwork provided, Sir Mark wanted to track back over the timeline, as there were gaps where the internal process and paperwork had not been properly completed. He expressed concern that there might be other examples and would like to be reassured that this was just an isolated example. The 2013 BPDAR was unsigned and he could see no evidence that this BPD had been brought to the BPD panel between 10/13 and 9/15. Since the briefer had taken on responsibility for the data, shortly before the inspection, it was now properly managed and deleted. A GCHQ official assured Sir Mark that new staffing would allow Mission Policy to work through all BPDs to track if there were other cases. Sir Mark was content for any other cases to be brought to his attention at inspection, not as they occurred or were discovered. As a result of this the Mission Policy compliance team reviewed all BPD paperwork to ensure that there were no further oversights on documentation – and to highlight any areas of non-compliance It was also agreed that Sir Mark should receive minutes of the BPD panel meetings with the choice letter for each inspection.

98. Sir Mark was informed that another BPD was now being removed from the main corporate BPD tool as the system was being decommissioned. The team had received permission to put this data onto another system.

99. The final BPD inspected was one that was proactively raised with Sir Mark to explain an error in our internal handling. This was a copy of a dataset released openly and publicised by the online media organisation "The Register". It claimed to contain the names and photos of several thousand intelligence officers. GCHQ's Operational Security team took a copy in case the material was no longer available, in order to check for any GCHQ names. As GCHQ was the only agency having access to the information on

classified IT systems, MI5 and SIS requested a similar search against their own staff list. Relevant information was also shared with a 5-Eyes partner Agency. The internal error consisted of not originally asking for authorisation to share with the other two UK Agencies and the foreign partner. After discussion with Mission Policy retrospective authorisation to share had been granted. Though the data had by then been deleted, there was an ongoing requirement to repeat the exercise as the public dataset was likely to be populated with further releases.

100. In relation to the latter BPD, Sir Mark commented that this was in a different category to other work we do and to other BPDs. Defence of employees was justifiable and it made use of a capability we possess. It was right to go through the BPDAR process but there was no question about it being the right thing for us to do, including sharing with our partners. This was a defensive not offensive activity.

101. I exhibit as GCHQ2 the Confidential Annexes to the reports of the Intelligence Services Commissioner for 2010 onwards.

Instances of non-compliance with safeguards relating to BPD

102. There have been three examples of non-compliance where BPD has not been handled in accordance with our internal policies since 2010. The first case concerns a BPD which was acquired in 2012. The acquisition was approved, and the relevant BPDAR signed. However, the dataset was not subsequently reauthorized or considered by the BPD Review Panel, as was required. This oversight was discovered in 2015 by GCHQ's Compliance Team, who then contacted the 'owners' of the dataset. The dataset was deleted in August 2015 as it was deemed to be no longer of use. According to GCHQ's audit logs, no queries had been run against this dataset after its initial acquisition was authorised.

103. The second case was a BPD which was first acquired by GCHQ in 2010. However, it was not initially recognised by GCHQ as a BPD. GCHQ's acquisition of this data pre-dated the current BPD process and the acquisition and retention of this data was initially approved under the Mission Policy Legalities-approved mechanism at the time for the standard 2-year retention period for operational data. It was subsequently identified as BPD in 2015 by GCHQ's Compliance Team in the context of using the data for training purposes. It was then brought within the BPD regime and subjected to the relevant safeguards, forms and oversight.

104. The third case is that described in paragraph 99 above. This case was not referred to in the Response to Request for Further Information which addressed non-compliance in respect of BPD. It was unfortunately overlooked because the Commissioner, who was aware of the case, had not requested any remedial action. However, it fell within the terms of the Request for Further Information and therefore should have been mentioned.

105. There have been no instances of deliberate misuse of BPD by GCHQ staff members.

PROPORTIONALITY

106. I have explained above the essential importance of BPD to GCHQ (and indeed to the Intelligence Services' operations generally) and also how it enables the identifications of individuals of intelligence interest without having to use more intrusive investigative techniques. I set out below a number of examples of the usefulness of BPD in this regard.

107. **Focusing investigative resources.** Intelligence indicated that a partially identified associate of a known subject of interest aspired to travel to Syria for extremist purposes. Using BPD, agency analysts were quickly able to identify the associate, enabling rapid focus of investigative effort on the one individual of concern and discounting hundreds of other potential candidates. Without access to BPD, a resource intensive and more intrusive process would have been needed to identify the individual from the hundreds of potential candidates, incurring collateral intrusion into individuals of no intelligence interest and with significant risk of failing to identify the individual prior to travel.

108. **Stopping Al Qaeda (AQ) terrorist plots.** Intelligence received by the Intelligence Services indicated that a member of AQ was facilitating suicide bombers in the UK. The Intelligence Services had a broad description for the AQ member but no name. Potential contact information was received, but didn't immediately identify the individual. Using BPD analysts were able to identify possible matches and quickly narrow this down to one strong match. At this point the necessity and proportionality case was robust enough to deploy other, more intrusive methods to cross-check the information and positively identify that the match was the suspected AQ member.

109. **Identifying foreign fighters.** Timely access to travel data has provided advance notice of the unexpected return to the UK of people judged to pose a potential threat to UK security. This helps the Intelligence Services to prepare a tailored response prior to their arrival to better mitigate the threat they pose to national security. Information derived from travel data has also been critical to the ability of the Intelligence Services and their international partners to identify individuals travelling to join Daesh in Syria and Iraq and then disrupt their activities, including when they return to the UK radicalised.

110. **Identifying subjects of interest.** The name of an individual reported to be storing a weapon used in a terrorist attack was identified by the Intelligence Services. A combination of BPD were used to fully identify this person from hundreds of possible candidates. This resulted in the recovery of the weapon, and aided in the subsequent conviction of the individuals involved in the terrorist attack, who are now serving lengthy prison sentences.

111. **Preventing terrorist access to firearms.** The risks of terrorist access to firearms have been highlighted by tragic events in Mumbai, Copenhagen and more recently Paris. To help manage the risk of UK based subjects of interest accessing firearms, the Intelligence Services match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the Intelligence Services acquired multiple datasets that contained the details of individuals who may have access to firearms, even though the majority will not be involved in terrorism and therefore will not be of security concern. This allows the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. This in turn has enabled the Intelligence Services to manage the associated risks to the public.

112. **Identifying human intelligence agents.** The Intelligence Services were tasked by the UK's Joint Intelligence Committee to produce intelligence on a specific country threatening the UK's national security. They identified an individual with access to the required intelligence, but were unable to approach the individual directly due to the risk the individual would face from his country's own internal security service. Intelligence reporting showed that the individual was in contact with another person that the UK agencies might be able to approach with lower risk. The reporting, however, did not fully identify who this contact was. The security and intelligence agencies used BPD to identify that contact conclusively, enabling them to determine that they could safely approach the contact and seek support. The contact has been successfully recruited as an agent to help collect intelligence and protect the UK's national security.

113. **Protection of major events.** When significant events take place - such as the NATO Summit in Wales in 2014 or the London Olympics in 2012 - the Intelligence Services work to ensure they occur safely. This includes tracing the details of individuals with access to venues so as to mitigate the risk that subjects of national security interest might gain access to these events. The majority of individuals in such datasets will not be of direct intelligence interest and this data is therefore treated as BPD.

114. Without using this information, it would be far harder, more costly and intrusive for the police and agencies to put in place alternative measures to provide security assurance.

C. BULK COMMUNICATIONS DATA ACQUIRED USING SECTION 94 TELECOMMUNICATIONS ACT

115. Communications data is of critical value to GCHQ. Obtaining and analysing such data enables the identification of patterns of communications that indicate potential threats to national security and the discovery of potential subjects of interest. The specific value of communications data obtained from CSPs under section 94 directions is that it provides more comprehensive coverage than is possible by means of interception

under section 8(4) of RIPA. Such interception can only provide coverage of a very small fraction of external communications due to the way in which communications are routed over the internet. By obtaining communications data pursuant to section 94 directions GCHQ is able to provide a higher level of assurance that it can identify e.g. patterns of communications than it could by means of interception alone.

116. It is also important to note that as a result of identifying patterns of communication and potential subjects of interest through obtaining and analysing communications data, it is possible to focus on specific individuals, and thus significantly reduce the intrusion into the privacy of individuals of no intelligence interest.

117. GCHQ first used a Direction under s.94 to obtain Communications Data in bulk in March 1998.

118. On 1 March 2001 GCHQ sought and obtained three new Directions under s.94.

119. GCHQ carried out call records research (supported by directory information) in response to specific queries from intelligence customers. Typical requests involved the identification of subscribers and of new telephone numbers for known subscribers; post-incident analysis, aimed at identifying individual subjects of interest; and support to agent handling. In addition GCHQ used call records research to identify relevant new telephone numbers, which could then be targeted for interception.

120. GCHQ expected the data to contribute significantly to intelligence on other subjects. It would potentially allow GCHQ to:

- Tip off Security Service or law enforcement agencies when a subject of interest had arrived in the UK;
- Provide intelligence on the UK contacts of a visiting subject of interest;
- Identify the telephone number of a visitor already under surveillance by Security Service, allowing them to seek an interception warrant while he was still in the UK.

121. GCHQ's s.94 Directions were updated and expanded in late 2001 following the 11 September attacks in the US.

122. Since 2012 GCHQ also requests Internet Communications Data to enhance UK cyber defence operations. The first request for this data was in support of the 2012 Olympics

D. SAFEGUARDS AND OVERSIGHT MECHANISMS FOR SECTION 94 BCD

123. GCHQ's use of BCD and of Section 94 of the Telecommunications Act 1984 to acquire BCD, like all areas of GCHQ's operational activity, is, and has throughout the entire period with which this claim is concerned been subject to the safeguards set out in GCHQ's Compliance Guide.

124. As noted in paragraphs 31 to 33 above, in the period June 2005 to 2010 the relevant version of the GCHQ Compliance Guide was the document exhibited at pages 89 to 146 of Exhibit 'GCHQ1'. In the period 2010 to June 2014 the relevant version of the GCHQ Compliance Guide, as amended from time to time, was the document exhibited at pages 147 to 162 of Exhibit 'GCHQ1'. In the period June 2014 to the present the relevant version of the GCHQ Compliance Guide, as amended from time to time, is the document exhibited at pages 5 to 24 of Exhibit 'GCHQ1'.

125. The Compliance Guide provided, and continues to provide, overarching safeguards relating to the requirements that all operational activity must be authorised, necessary and proportionate and guidance as to those requirements, as well as specific guidance in relation to specific areas of operational activity.

GCHQ Section 94 Handling Arrangements

126. On 4 November 2015 the GCHQ Section 94 Handling Arrangements, made under section 4(2)(a) of the Intelligence Services Act 1994, came into force. A copy of the GCHQ Section 94 Handling Arrangements is exhibited at pages 81 to 88 of exhibit "GCHQ1". These set out detailed provisions (which are not repeated here) in relation to the acquisition and use of section 94 data.

Audit

127. Access to bulk communications data requirements the completion of Necessity and Proportionality statements. These are subject to the same audit arrangements as described in paragraph 60 above in relation to BPD.

TRAINING ON SECTION 94 BCD WITHIN GCHQ

128. Within GCHQ data acquired under s.94 Directions is handled in the same way as related communications data obtained under s.8(4) RIPA warrants. It is held in the same databases. When an analyst seeks to query communications data the query will be run against data obtained from both sources and it will not be immediately apparent to the analyst which source provided what parts of the response to the query. For this reason there is no specific training on the handling of data obtained under s.94 Directions.

129. In order to be granted access to GCHQ systems that hold communications data, all analysts must take and pass the MLO and AML training described in paragraphs 62 to 65 above. They must also meet the specific requirements for the particular system or tool that they wish to use. These requirements will typically be expressed in terms of a minimum skill level in the appropriate analytical techniques, and/or a business case endorsed by a manager in the analyst's local area, and the relevant tool- or system-related training.

130. As an example of how this works in practice, I will describe the process for applying for access to the main system developed by GCHQ for the storage and retrieval of bulk telephony and bulk internet data. This holds data obtained under s.94 directions and obtained as a result of interception under RIPA s.8(4), which has been automatically processed and indexed to allow it to be queried at operational pace. There are three types of accounts on this tool: Level 1, Level 1+ and Level 2. As the level increases, so does the functionality available to the account holder. For instance at level 2 an analyst has the capability to access communications content through the tool, subject to additional legal and policy controls. A Level 1 account holder is unable to do this.

131. If an analyst seeking an account on the system does not yet have a validated analytic skill (e.g. network analysis, mobile and telephony analysis or access and intelligence mission management) then they need to draw up a business case for a Level 1 account. This case must include: confirmation that the analyst has completed and passed AML training; confirmation that they have a job requirement to use the data held in the system; and confirmation that there are people within the analyst's business unit who will support the analyst in their learning and development and in their use of the system. This case must be approved by a local manager at a defined minimum seniority level (the level is higher for accounts granted to integrees from other agencies or contract staff). Either the application or the approver's comments must briefly cover the analyst's role and how they will be using the system (e.g., "As an X working in Y team I will need access to the system to do Z") and how they will be supported in their team (e.g. "I sit with colleagues who are system users" or "We have a senior technical analyst who can help me with any queries related to the system").

132. Once completed and approved by the local manager the application is sent for review by the senior user community for the system who have final sign-off. If they approve the case then the analyst must read the defensive brief for the system, which:

a) summarises what the system does;

b) reminds the analyst of the requirement to consider the proportionality of their use of the system;

c) sets out the policy requirements related to certain types of query and the implications of non-compliance with the rules for such queries; and

d) provides points of contact for further advice.

133. The analyst may then apply to the IT services account management system for their account, and once it is active, complete the specific on-line training for the system. Once the account is operational it must be used at least once every six weeks or it will expire and a new application will be needed.

134. If the analyst already has an up-to-date and validated qualifying skill then they need not make a formal business case. They must however have completed the AML training and have read the defensive brief. They may then apply to IT services and must take the on-line training as described in paragraph 133 above. In practice however it is difficult to achieve the necessary skill levels without access to this particular system.

INDEPENDENT OVERSIGHT

135. In 2004 Sir Swinton Thomas agreed to provide non-statutory scrutiny over section 94 directions, and the applications for those directions. His scrutiny began in 2004 and continued until 2006 when Sir Swinton ceased to be Interception of Communications Commissioner.

136. In 2004, following exchanges between the Home Office and Sir Swinton Thomas over MI5's use of section 94 directions, GCHQ also wrote to Sir Swinton explaining the safeguards we applied to access to bulk communications data acquired through a section 94 direction. Copies of that correspondence are exhibited at pages 175 to 182 of exhibit "GCHQ1".

137. When Sir Swinton finished his term as Interception of Communications Commissioner in 2006, Sir Peter Gibson, the Intelligence Services Commissioner, agreed to provide non-statutory scrutiny of section 94 directions, and the applications for those directions.

December 2010

138. Sir Peter Gibson reviewed retrospectively a request to a CSP for specific data obtained by GCHQ under section 94 of the Telecommunications Act 1984. We explained that we were aiming to reduce the number of data holdings that were not under judicial oversight, and envisaged that all data holdings (including those under s.94) might eventually come under a Code of Practice and statutory oversight arrangements. Sir Mark Waller, who as noted in paragraph 67 above was due to replace Sir Peter as

Intelligence Services Commissioner, and accompanied him on this inspection, agreed that he would in principle be happy to oversee such requests in the future.

139. Sir Peter was satisfied both with his review of the relevant submission and instrument, and with a short presentation on the benefits of this data, particularly in the context of counter-terrorism operations.

March 2011

140. Sir Mark Waller visited GCHQ on 1 March 2011 for a familiarisation visit. While there was a session during which Sir Mark was able to discuss and finalise his selection of BPDs and s.94 Directions ahead of his first formal inspection there was no substantive discussion of s.94 Directions.

141. The formal inspection took place on 29 March 2011. Sir Mark had selected one s.94 Direction for inspection. We provided a briefing on the two sets of data provided under the Direction. Any searches of the data were logged and auditable. Sir Mark was satisfied with the case for acquiring and retaining the data, commenting that most people would assume such data was available to security and intelligence agencies.

October 2011

142. Sir Mark Waller conducted an inspection on 17-18 October 2011. He looked at one s.94 Direction. We described how samples of rich communications data had been obtained. Sir Mark was interested in where the data was stored: being telephony communications data this was stored in a corporate database along with a larger portion of RCD obtained from RIPA 8(4) collection. Sir Mark was interested in how access to this data was controlled, and how audits were performed and potential misuse might be found. There was some discussion of how far it might be reasonable to provide a report to Sir Mark on this aspect when the majority of the communications data subject to these controls would be acquired in the course of warranted interception and therefore under Sir Paul Kennedy's remit. Although Sir Mark had agreed to oversee the s.94 data in response to GCHQ's request rather than for any other reason, his interest was at least as much in monitoring of potential misuse as in the justification for acquiring the data.

March 2012

143. Sir Mark Waller conducted an inspection on 19-20 March 2012. He was content with the one Section 94 Direction that he inspected. His only comment was that he would have liked to have seen a more explicit assertion that GCHQ would only search the data for its lawful purposes, in addition to the words on proportionality that appeared in the 'Legal Issues' section.

December 2012

144. Sir Mark Waller conducted an inspection on 4-5 December 2012. He examined one Direction under s.94 of the Telecommunications Act. The Commissioner pointed out that the application for the direction was on the basis of a nine month pilot proposed in April 2007, but we were still getting access to the data some years on. It was explained that s.94 Directions did not expire, and there was no provision in the Act to renew them. In this case GCHQ had reported back to the Foreign Secretary in January 2008 on the pilot and confirmed that they wished to continue to receive data for operational use under this Direction. We explained that GCHQ would resubmit for a direction if a company changed its name. We added that we also review the requirements for data under each Direction every 6 months and write to the company concerned to inform it that we continue to require the data.

145. Sir Mark appeared reassured that the data could only be queried if an HRA justification has been supplied by the querying analyst. He sought and was provided with clarification on the type of reporting that was derived from this data.

June 2013

146. Sir Mark Waller conducted an inspection on 4-5 June 2013. He examined one s.94 Direction. Sir Mark explained that he was particularly interested in the necessity and proportionality of GCHQ acquiring data under s.94 and he was interested in the possibility that the data we acquired under this authority included information that was private. He asked that, when seeking a Direction, the submission should include more specific information covering privacy safeguards and providing further evidence that the expected intelligence gains outweighed the level of intrusion.

December 2013

147. Sir Mark Waller conducted an inspection on 10-11 December 2013. He inspected one s.94 direction. The Deputy Director for Legal Affairs reminded him of the background to s.94 directions. As s.94 directions have no expiry date, it was explained that the requirement for the data was reviewed every six months and the company informed of the continuing requirement or a decision to discontinue the provision of the data, as appropriate. Some companies preferred to be informed orally rather than in writing as they did not have storage facilities for highly classified documents.

148. Sir Mark requested that confirmation of the outcome of the latest review be included in the reading pack for selected s.94 directions. This should either be a copy of the letter sent to the company or a note of when the oral confirmation of the continuing requirement was made to the company.

May 2014

149. Sir Mark Waller conducted an inspection on 28-29 May 2014. Our records of this inspection are very limited, however it is clear that no action was required by Sir Mark following his inspection.

November 2014

150. Sir Mark Waller conducted an inspection on 11-12 November 2014. He examined one s.94 Direction. He asked to see the covering note to the Foreign Secretary relating to the most recent review, plus a copy of the letter to the CSP.

151. The Prime Minister wrote to the Interception of Communications Commissioner in January 2015 to ask him to extend his oversight to directions given by a Secretary of State pursuant to section 94 of the Telecommunications Act 1984 in respect of bulk communications data.

May 2015

152. Staff from the Interception of Communications Commissioner's Office (IOCCO) conducted an inspection on 6 May 2015. There was some discussion of s.94 authorisations in the context of the oversight of Sir Anthony May, at that time the Interception of Communications Commissioner. IOCCO queried why GCHQ and MI5 had different approaches to safeguards at the stage of access to section 94 data. I was present at this inspection and I explained that this was because the approaches were aligned to each agency's respective primary activities in relation to communications data. MI5 also obtained communications data via Part I Chapter II requests whereas the vast bulk of GCHQ's communications data is obtained via 8(4) interception. Our approaches to acquisition and use of data obtained under s.94 merely reflected organisational differences.

November 2015

153. Staff from the Interception of Communications Commissioner's Office conducted an inspection on 26-27 November 2015. We provided a background briefing on GCHQ's use of Directions issued under s.94 of the Telecommunications Act 1984.

Instances of non-compliance with safeguards relating to section 94 BCD

154. There have been no instances of non-compliance at the acquisition stage in respect of communications data obtained under section 94. Although any instances of non-compliance in respect of access to bulk communications data will have been identified and reported to the Commissioner, it is impossible to ascertain whether any such

instances concern data obtained under section 94 or data obtained pursuant to a section 8(4) warrant.

PROPORTIONALITY

155. I have explained above the essential importance of communications data obtained by section 94 to GCHQ (and indeed to the Intelligence Services' operations generally). I set out below a number of examples of the usefulness of communications data in this regard.

156. **Preventing bombings in the UK.** In 2010, a group of terrorists were plotting bombings at several symbolic locations in the UK, including the London Stock Exchange. Following an intensive investigation, in which analysis of bulk communications data played a key role, not least as the network was spread across multiple locations, the group were all identified and their plot uncovered. The investigation required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data.

157. The Intelligence Services were then able to work with police to disrupt them in time and the group were charged with terrorism offences, including conspiracy to cause an explosion. All entered a guilty plea and were sentenced to prison terms of up to 18 years.

158. **Detection of ISIL attack planning.** In 2014, GCHQ analysis of bulk communications data uncovered a previously unknown individual in contact with an ISIL-affiliated extremist in Syria who was suspected of involvement in Western attack planning. Despite attempts by the individual to hide his activity, GCHQ was able to use bulk communications data to identify that he had travelled to a European country and separate intelligence suggested he was progressing with attack planning. The information was passed to authorities in that country, enabling the successful disruption of the attack planning. During the disruption several home-made IEDs were found.

159. **Preventing mass casualty attacks against aviation.** In 2006 a group of terrorists based in more than one part of the UK plotted to bring down multiple aircraft using homemade bombs (improvised explosive devices). If successful, their plan would have been the largest terrorist attack ever to take place in the UK, with a death toll similar to the 9/11 attacks in the United States. The Intelligence Services used bulk communications data to find these terrorists and disrupt their plan. This required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data.

160. Those planning the attack were arrested, tried and sentenced to life imprisonment.

161. **Disruption of child sexual exploitation (I).** GCHQ used analysis of bulk communications data to track down two men overseas who had been blackmailing hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. GCHQ analysts were able to confirm the suspects' names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.

162. **Disruption of child sexual exploitation (II).** Using bulk data to spot patterns of behaviour demonstrated by paedophiles, in 2013 GCHQ identified a UK national using paedophilic sites that required a payment to access the most extreme indecent images. This individual had previously held a position that provided him with access to children (and was on the Violent and Sexual Offenders Register). He was sentenced to 3 years imprisonment and made subject to a Sexual Offenders Harm Order for life.

Statement of Truth

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

GCHQ Witness

Dated: 8 July 2016

Amendments are double-underlined

Witness: MI5
Party: 4th Respondent
Number: 1
Exhibit: MI5 1
Date: 8.7.16

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

AMENDED WITNESS STATEMENT OF MI5 WITNESS

I, MI5 WITNESS, Deputy Director in the Security Service, of Thames House London SW1, WILL SAY as follows:

1) I have worked for MI5 for 25 years and have been a Deputy Director in the Security Service since 2010 and a member of the senior management group since 2004. I was Deputy Director for Data Access and Policy from 2013 to 2016. I have now (as of 4 April 2016) moved to be Deputy Director for Counter Terrorist Policy and Capability.

2) I am authorised to make this statement on behalf of MI5. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within MI5.

3) In my Data Access and Policy role I had substantial experience in relation to MI5's bulk communications data capability and, in the last year, also in relation to MI5's bulk personal data capability.
4) In this witness statement, and on behalf of all of the Respondents to this claim, I also address the current intelligence picture.

5) Exhibited to this witness statement is a bundle of documentation marked "MI5 1". References in this statement to page numbers (eg [pages xx to xx]) are to the page numbers of MI5 1.

SECTION 1 - THE CURRENT INTELLIGENCE PICTURE

THE CURRENT THREAT PICTURE IN THE UK

6) The governments of democratic states are charged with the duty of upholding the criminal law and protecting their citizens from threats such as organised crime and terrorism. The UK has for many years faced a serious threat from terrorism. Over recent years, the threat to the UK from international terrorism in particular has continued to increase.

7) Some of the key events over the period since 2005 that illustrate the nature of the threat from international terrorism, are:

   a) Following 9/11, Al Qaida (AQ) was the leader of global jihad through the 2000s. The group posed the greatest threat to UK and Western interests at home and overseas with its ability to direct terrorist attacks in Western countries, as seen in the 7/7 London transport attacks and the failed transatlantic airliner plots in 2006.
   b) An attack in 2007 targeted a London nightclub, followed by Glasgow International Airport, while in 2009 we saw a sophisticated attempt to bring down an airliner with a non-metallic bomb hidden in underwear.
   c) Since the beginning of the Syrian conflict in 2011 the threat from Near East has grown significantly. Western foreign fighters travelled to Syria initially to join AQ's affiliate al Nusrah Front - that group now being AQ's most effective affiliate. Daesh, borne from AQ in Iraq, have had a meteoric rise since declaring a caliphate in 2014.
   d) Daesh's attacks against Westerners in Tunisia in June 2015, Paris in 2015 and Brussels in 2016 proved their external operations capability; their Sinai branch's attack against the Russian airliner in October 2015 demonstrated their ability to mount a complex, mass-casualty attack against Western aviation. As such, Daesh continues to pose the greatest threat to the UK homeland and our equities overseas, with its ability to inspire, enable and direct attacks around the world.

8) In August 2014, the UK threat level, assessed independently by the Joint Terrorism Analysis Centre ("JTAC"), was raised to "SEVERE" from "SUBSTANTIAL", which means that an attack in the UK is highly likely. The international terrorist threat to the UK continues to be dominated by the ongoing conflict in Syria and Iraq and the ability of terrorist groups there to inspire, enable and direct Islamist extremists to conduct attacks around the world, including in the UK. Attacks could be undertaken by extremists living in the UK, as was seen with the 7/7 London attacks, or by foreign nationals travelling to the UK for terrorist purposes. The Government introduced new legislation (the Counter-Terrorism and Security Act 2015) to ensure that the SIA has the appropriate legal powers and capabilities to tackle international terrorism, including the ability to stop people travelling to fight in conflict zones like Syria.

9) The 2014 Annual Report by the Home Office on the UK's Counter-Terrorism Strategy ("the CONTEST Report") [pages 319-344] , published on 23 March 2015[1], highlights the increase in the frequency of terrorist incidents around the world, and the number of fatalities associated with such attacks. The Report explains:

"The principal threat continues to come from militant Islamist terrorists, notably in Syria and Iraq. ISIL [Daesh] and other terrorist groups in Syria are now supported by foreign fighters from the UK and other European countries. About 600 people with extremist connections are among the many Britons who have travelled to the region from the UK. Many have now returned here. Some are likely to have received combat experience and other terrorist related training. Terrorism is being fuelled by an unprecedented quantity of extremist and terrorist propaganda."

10) According to the Global Terrorism Index[2] [pages 345-456], in 2014 (the latest year for which published statistics are available) there were over 32,000 deaths across 67 countries from terrorism; 78% of these deaths occurred in just five countries – Iraq, Nigeria, Afghanistan Pakistan and Syria. The Index also confirms that the flow of foreign fighters to Syria continues, with current estimates suggesting 25,000-30,000 fighters from 100 different countries have travelled to Syria and Iraq since 2011. It is estimated that over 7,000 new fighters travelled to Syria in the first half of 2015. It reports that 21% of those fighters travelled from Europe. This highlights the continuing appeal of the conflict in Syria, and the strong enduring appeal of groups like Daesh.

---

[1] The 2016 report is presently being updated by the Home Office and will be published in July 2016.

[2] Global Terrorism Index 2015, Institute for Economics & Peace

11) On the 17 September 2015, Andrew Parker, the Director General of the Security Service (DG for MI5), during an interview with the BBC [pages 457-462], revealed that six alleged terror plots targeting the UK had been stopped in the preceding twelve months.

12) However, the murder of two British and other hostages in Syria (apparently by a member of Daesh closely connected to the UK), recent terrible events in Paris (the attacks of January and November 2015) and the 31 Britons killed in the attacks of March and June 2015 (on a Tunisian museum and beach resort), have underlined the threat posed to British nationals - not just in Syria or Iraq - but also outside those arenas, including within the EU. Even more recently, on 22 March 2016, Daesh conducted a coordinated terrorist attack at two locations in Brussels killing 35 people and injuring a further 270. Daesh claimed responsibility for the attack via a Daesh-linked media outlet later the same day. In the weeks following the attack the two surviving perpetrators were arrested and remain in custody.

13) There remains, also, a threat from Northern Ireland-related terrorism. The threat in Northern Ireland is assessed by MI5 to be "Severe", meaning that a terrorist attack is assessed to be highly likely. The threat from Northern-Ireland related terrorism to Great Britain was recently raised (on 11 May 2016) from "Moderate" to "Substantial", meaning a terrorist attack is a strong possibility.

14) Serious and organised criminals, terrorists and others who may seek to harm UK national security frequently operate and co-operate across national borders. Further, such individuals frequently seek to plan, prepare for, coordinate or carry out activities that are designed to harm UK interests whilst they are outside the UK, or in association with others who are outside the UK.

15) As regards the threat from international terrorism, the CONTEST Report noted in this regard at paragraph 1.3 that:

"Although some terrorist plots here are developed entirely by British nationals living in this country, many of the threats we face continue to have significant overseas connections."

16) Whilst Daesh continues to inspire groups and individuals around the world, and threaten Western equities in those countries, they are not the only group posing a truly global threat. Al Qaida (AQ) remain a potent, global, terrorist organisation. Al Nusrah Front in Syria is now AQ's most effective affiliate. AQ in the Islamic Maghreb, with their recently re-joined splinter group Al Murabitun, continues its terrorist activity across North Africa, as seen in their attack on 20 November 2015 against the Radisson Blu Hotel in Bamako, Mali. Whilst Daesh has captured more press headlines in recent years, AQ continues to have the intent and capability to attack Western interests, including UK interests, across the world.

17) The threat to the UK does not stem just from terrorism.

18) Regional conflicts and the aggressive behaviour of authoritarian regimes pose an increasing threat to the UK. Foreign intelligence agencies continue to engage in hostile operations against UK interests. This includes gathering sensitive intelligence on a broad range of subjects in the UK, including foreign policy, defence, energy, financial, technological, industry and commercial interests. Some hostile services also pose a threat to the physical security and safety of UK citizens or residents. The most capable foreign intelligence services seek to use a full spectrum of capabilities - including SIGINT, cyber and technical operations - in order to undertake these activities.

19) The Government also regards serious and organised crime as one of the most significant threats to the UK. The National Crime Agency is responsible for the investigation of serious organised crime and published a strategic assessment of serious and organised crime on 23 June 2015 [pages 463-510]. MI5 works closely with the NCA and the Police on a range of issues, and GCHQ supports the NCA's work in particular on online crime and Child Sexual Exploitation.

20) The threat from serious crime to the UK is wide ranging. Law enforcement agencies and policy departments task (and SIA partners collaborate) as to their respective requirements from the SIA in relation to the serious crime threat. These range from tactical intelligence providing operational leads and capability development, to intelligence illuminating the scale and nature of strategic threats from Cybercrime, CSEA, financial crimes, drugs trafficking, firearms smuggling and illegal people smuggling and trafficking. Combined, these threats are assessed by Home Office to amount to a National Security threat to our security and economic stability, with billions of pounds worth of financial crime, health threats from Class A drugs, political issues such as illegal immigration and the potential CT threat from leaving our borders vulnerable to extremists and firearms.

21) As criminals are not confined to any particular part of the world, this threat can emanate from anywhere. Most frequently the organised crime groups we produce intelligence on are networks of individuals spread around different parts of the world, or situated in inaccessible places. The SIA seek to combine all available intelligence gathering techniques to find the pieces of the jigsaw puzzle, particularly when the activity is conducted in parts of the world which do not otherwise appear on national strategic priority lists.

CHALLENGES FACED BY THE SIA IN TERMS OF THE CURRENT THREAT

22) The task of defending the UK's interests and protecting its citizens from the threats outlined above has become increasingly complicated and challenging in the age we live in. The evolution of the internet and modern forms of communications are providing terrorists and criminals with new ways to plan direct and increasingly execute their plots. The CONTEST Report notes that Daesh in particular is using social media "....in an unprecedented quantity and frequency, including personalised messages from UK and other foreign fighters and propaganda from the organisation." As the DG for MI5 explained in a public speech to the Royal United Services Institute (RUSI) on 8 January 2015 [pages 511-524] :

"It makes full use of the modern social media and communications methods through which many of us now live our lives. By these means it spreads its message of hate directly in to homes across the United Kingdom - both to those seeking it and those who may be susceptible to its distortion and glamorisation of horrific acts".

23) Robert Hannigan, the Director of GCHQ also drew attention in November 2014 [pages 525-526] to the way in which Daesh is using the internet to "create a jihadi threat with near-global reach". In particular:

"[Daesh] also differs from its predecessors in the security of its communications. This presents an even greater challenge to agencies such as GCHQ. Terrorists have always found ways of hiding their operations. But today mobile technology and smartphones have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are "Snowden approved". There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years."

24) The diversification of the communications market and the ability of terrorists, criminals and others to exploit new internet-based technologies has made it increasingly difficult for the SIA to monitor the communications of those who present a threat to UK interests. Unless the intelligence services are able to maintain their capabilities in the face of these unprecedented technological challenges, the UK will be unable to obtain the intelligence it needs to counter these threats. As the Chief of SIS made clear in his speech to English Heritage in March 2015 [pages 527-536], the SIA is engaged "... in a technology arms race".

25) The use of communications data (the who, where, when and how of a communication but not its content) is a vital tool in the investigation of threats and safeguarding the public. The DG for MI5, discussed the importance of communications data in meeting the challenges that the SIA face in his BBC interview of 17 September 2015 [pages 457-462]:

"We need to be able to use data sets so we can join the dots, to be able to find and stop the terrorists who mean us harm before they are able to bring the plots to fruition. We have been pretty successful at that in recent years but it is becoming more difficult to do that as technology changes faster and faster."

26) However obtaining communications data in the digital age is getting harder. In a public speech given to RUSI on 10 March 2015 [pages 537-542], the Foreign Secretary offered a summary of the challenges posed by the accelerating pace of technological change:

"And as the range of threats gets bigger, so the pace of technological change with which the Agencies must keep pace is getting faster, making their central task of keeping us safe ever more demanding. The Agencies have always had to innovate to stay one step ahead of their adversaries. But the accelerating pace of technological change has upped the ante as terrorists, states and others who would do us harm embrace, adapt, and abuse the technology that we so readily welcome in our everyday lives.

And it is a truism that as technology enables greater productivity, it also open us up to greater vulnerability. So our Agencies must master every technological advance. They must understand its strengths, its weaknesses, the vulnerabilities it introduces – before our enemies can turn it against us".

27) David Anderson QC also highlighted the impact of these challenges at paragraph 2.14 of his annual report on the operation of the Terrorism Acts (September 2015) [pages 543-626]:

"It has been a feature of several major terrorist attacks, including the 7/7 bombings, the killing of Lee Rigby and the French shootings in January 2015, that one or more of the perpetrators was known to the police or security services but had not been assessed as posing a major risk at the time. The speed with which things can change, and the difficulties in knowing how best to prioritise limited surveillance resources, were illustrated in unprecedented detail by the inquiry of Parliament's Intelligence and Security Committee into Lee Rigby's killing."

28) One of the key technological challenges currently faced by the Agencies is that of encryption. Whilst encryption provides a means of making sure that communications cannot be read by anyone other than the intended sender or recipient, the same technology can, and is, used by terrorists and serious criminals to carry on their activities undetected. The spread of encryption has been positive for businesses and citizens, but, has also had implications for the Agencies in pursuing their work against those who intend to cause the country harm.

29) The proliferation of online Secure Messaging Applications means that terrorists are able to use SMAs to encrypt their communications as well as anonymisation software to mask their online identity. When used consistently and correctly, the anonymisation and security these applications provide make it difficult for the intelligence and security agencies to identify attack operatives or attack plans.

30) The external threat to the West from Daesh's online activity comes from: a sophisticated media strategy inspiring attacks; online methodology guidance enabling attacks and extremist travel; Syria-based foreign fighters inciting attacks and senior leadership directing external attacks. Daesh's overt use of social media and covert use of secure messaging applications and anonymisation software are key to progressing all areas of this threat.

31) As the Government set out in the 'Operational Case for Bulk Powers' published alongside the introduction of the Investigatory Powers Bill in March 2016 [pages 627-674], the growth in the availability of encrypted communications has had two implications for the security and intelligence agencies;

"First, they have had to become less reliant on obtaining the content of a suspect's communications: when investigating a known threat in the UK, the agencies will often have to make greater use of bulk data to identify associates and to reveal possible attack planning. Second, the ability to obtain the communications of suspects overseas increasingly requires the use of equipment interference in order to supplement bulk interception."

32) In the 2015 Spending Review (published on 27 November 2015) [pages 675-784] the Government set out its intention to "protect the UK's national security by investing in defence, policing, intelligence, counter terrorism, cyber security and international aid, protecting British citizens at home and projecting British influence abroad". In line with this, the Government's Spending Review funds the Strategic Defence and Security Review in full "enabling the government to respond effectively to the strategic threats and opportunities that the UK faces". This includes allocating an additional £3.5 billion to a Joint Security Fund to 2021 to increase spending on the military and intelligence agencies, plus an investment of £1.9 billion in cyber security and £3.4 billion in new counter terrorism activity.

33) In the face of this significant and enduring threat from terrorism, serious and organised crime and other national security threats there is a pressing need for the SIA and law enforcement agencies to be able to secure valuable intelligence in order to pursue their statutory objectives. It is in this context that BPD and BCD are so important to the SIA. In particular and to the extent that we do not now receive information (that previously we could obtain) then such information as we derive from other sources, such as BPD and BCD, is that much more crucial.

SECTION 2 – BULK PERSONAL DATA

34) I turn to deal with matters relating specifically to MI5.

Background

Development of BPD

35) In considering the development and history of the use of BPD by MI5, it is important to recall that BPD is, ultimately, a categorisation of a certain type of data. In particular, BPD is not, in and of itself, a capability or a technique, in the way that for example interception or equipment interference are. The holding of information, for the purposes of national security, is one of the primary functions of MI5 (further to section 2(2)(a) of the Security Service Act 1989) and BPD is, ultimately, simply one of the categories of information (amongst others) that MI5 needs to hold in order to fulfil that statutory function.

36) The essential features of BPD (adopting the definition in the Prime Minister's direction of 11 March 2015 to the Intelligence Services Commissioner) [pages 785-786] are that it is a collection of data which:
- comprises personal data;
- relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest; and
- is held (or is acquired for holding) on the analytical systems of the intelligence agencies.

Why do we need BPD?

37) With the growth of digital technology and with the availability of a range of different datasets in an electronic format (such that the data could be put onto our analytical systems for the purposes of being combined/fused) it became increasingly obvious, during the early to mid 2000's, how vitally important, for investigations, the capability to use BPD was. The appreciation of the value of BPD also became apparent from particular investigations for which we had acquired particular datasets. For example, whilst in the first instance such

datasets may have been time limited in scope, because they related to particular investigations, it became apparent how a dataset of that type, which had been very useful for one investigation, had the potential to be enormously valuable for other investigations as well.

38) An early example of this appreciation of the value of BPD is an investigation which took place in late 2004 /early 2005. Sensitive intelligence suggested that an Al-Qaeda operative, identified only through fragmentary information, was a potential suicide operative in the UK. Based on a bulk dataset there were initially some 27,000 potential candidates. Through applying various filters to the dataset the number of candidates was reduced to approximately 3,000. Matching with another dataset reduced the number to 40, and finally matching with a third dataset (passport data), provided one match.

39) The significance of being able to combine (or fuse) data in an analytical system is that it enables common themes/points to be found quickly and efficiently in a way that is simply not possible through making individual searches of individual datasets. In particular, individual searches of separate datasets will result in a series of potential "answers". However, absent the ability digitally/electronically to combine datasets, the answers from searches on individual datasets would need to be manually checked across all the other relevant datasets. That is extremely labour intensive but, most significantly, can be very slow, and in an environment where quick answers are usually essential.

40) At the same time in the early 2000s, and in particular in the aftermath of the terrorist attacks in the US on 11 September 2001, it became increasingly common for MI5 to receive snippets of information relating to a threat that, on their own, did not tell us very much about the person, or people, involved. The ability to develop fragmentary intelligence into a real world identity has always been critical to intelligence work, and we realised that we needed to accelerate our ability to identify people from the intelligence that we were receiving. The use of BPD, and fused datasets, provided the capability to do this and to do so at speed and at a time when the threat required this. The value of this capability became even more significant following, in particular, the terrorist attacks in London in 2005.

41) Until mid-2007, the vast majority of BPD that MI5 acquired was held in an area of our analytical area of our systems where it was not generally accessible to investigators. More specialist analysts only (although they were often based in, and working closely with, investigative teams) had access to these areas. However, with the development of different platforms for analysis it became possible to make a number of the BPD datasets available to investigators more widely. The majority of our BPD datasets were kept (and still are today) on a part of our analytical systems, that specialist analysts only have access to.

However, as from mid-2007, a number of BPDs were made available, for the first time, to investigators more generally.

42) In view of: the increasing use and value of BPD within MI5; recognising BPD as a category of data in its right; and, in particular, because we proposed that some of our BPD would be made more generally available to investigators, we concluded that we ought to formalise the policy process by which datasets of this type were acquired and held, and reviewed, by MI5.

43) I refer further below (under "Safeguards") to the regime that we instituted in 2006 in order to achieve this. In formalising the acquisition and review process for BPD we also wished to recognise the legal context and the legal implications of the use and retention of BPD. As the 2006 policy document records, legal advisers within MI5 were - at that time - copied in on all reviews (for the retention of BPD) and the majority of the requests for BPD acquisitions.

What types of BPD are held

44) MI5 acknowledges that it holds the following categories of BPD:

- LEA/Intelligence. These datasets primarily contain operationally focussed information from law enforcement or other intelligence agencies.

- Travel. These datasets contain information which enable the identification of individuals' travel activity.

- Communications. These datasets allow the identification of individuals where the basis of information held is primarily related to communications data e.g. a telephone directory.

- Finance. These datasets allow the identification of finance related activity of individuals.

- Population. These datasets provide population data or other information which could be used to help identify individuals e.g. passport details.

- Commercial. These datasets provide details of corporations/individuals involved in commercial activities.

45) A number of these datasets will be available to the public at large. Some of these publicly available datasets will be sourced from commercial bodies and we will pay for them (as another public body or a member of the public could do). MI5 also acquires BPD from government departments, from SIS and GCHQ and from law enforcement bodies.

46) MI5's holding of passport information is key to our ability to be able to investigate travel activity. Holding that data in bulk, and being able to cross-match this to other data and other BPD held, is what enables us to find the connection and "join the dots". That would simply not be possible if we did not hold the bulk dataset in the first place. Using travel data, for example, to try and establish the travel history of a particular individual will necessarily involve holding, and searching across a range of BPD and other data that we hold, and it is through fusing these that we are able to resolve leads and identify particular individuals, with high reliability, at pace and with minimum intrusion.

47) Holding the data in bulk (and holding data relating to persons not of intelligence interest) is an inevitable and necessary pre-requisite to being able to use these types of dataset to make the right connections between disparate pieces of information. Without the haystack one cannot find the needle; and the same result cannot be achieved (without fusion/combination) through carrying out a series of individual searches or queries of a particular dataset (or a number of datasets).

48) It is also relevant to note that as BPDs are searched electronically there is inevitably significantly less intrusion into individuals' privacy as any data which is searched but which does not produce a "hit" will not be viewed by the human operator of the system, but only searched electronically.

Meaning of a sensitive dataset

49) All BPD, by virtue of its definition, comprises personal data (within the meaning of the Data Protection Act 1998 - DPA 1998) relating to individuals. However, our BPD processes recognise that some types of data can be more sensitive than others, because they may contain sensitive data.

50) MI5's current Handling Arrangements for BPD (item 21 of the RFI disclosure [pages 101-114 at page 102]) specifically cross-refer to the DPA 1998 definition of sensitive personal data (see paragraph 2.5) and the current acquisition form for BPD (V8 - item 6 of the 2005 to 2014/Historic disclosure [pages 83-88]) requires those seeking to acquire a dataset to identify whether the dataset contains sensitive personal data (referencing specifically: "*biometric, financial, medical, racial or ethnic origin, religious, journalistic, political, legal, sexual, criminal activity*").

51) Acquisition form V3-0 (see item 6 of the Historic disclosure [at pages 191/193]) referenced "sensitive data". Further, the 2010 BPD policy [page 8, 5th bullet] required investigators and managers, when assessing intrusion, to take into account whether "*the dataset contain sensitive personal information (e.g. relating to finances or medical conditions), albeit in a non-detailed format?*". Acquisition form V5-0 (in use as from approximately January 2011) [page 199] specifically asked

whether the dataset contains sensitive personal data (referencing expressly: *"financial, medical, religious, journalistic, political, legal"*).

52) In relation to medical data, I am able to confirm that MI5 does not currently hold, and has never held, a BPD of medical records. However, and as our forms for the acquisition of BPD recognise (see the foregoing paragraph), it is possible that data relating to medical conditions may appear in BPDs.

53) A sensitive dataset (as described above) is to be distinguished from a "high sensitivity dataset" as referred to, for example at [page 60] of the BPD guidance of November 2015 (at item 16 of the RFI disclosure). A high sensitivity dataset as mentioned here refers to a dataset from a particularly sensitive source and in particular, where this may have implications for how ongoing retention and review of that dataset is carried out within MI5.

54) In the event that the source is particularly sensitive or deemed "need to know" then the BPD internal guidance provides an alternative means for ensuring that the dataset is appropriately reviewed, albeit outside the usual review process (ie a more limited group of individuals, than the wider Bulk Personal Data Review Panel).

Meaning of corporate risk

55) The phrase "corporate risk" in this context refers to the potential for political embarrassment and/or damage to the reputation of MI5 and its SIA partners. MI5's BPD Guidance sets out [pages 64-67] how MI5 assesses the corporate risk associated with the acquisition of particular datasets and the standard acquisition form (section 5 of V8 [page 215]) requires this matter to be addressed.

Safeguards

As at 2006

56) As is apparent from the 2006 policy document "Bulk External Data Acquisition – Internal Authorisation Process" (item 4 of the Historic disclosure [pages 177-188]) the key issues that led to the development of this policy were that, outside of specialist areas within MI5, the then current bulk data request authorisation processes were not widely understood and bulk data requests were increasing in number. Accordingly, against that background (and a widening of access to some BPD for investigators), it was considered to be important that the policy process meant that each acquisition of BPD met a national security requirement (validated by MI5 management) and that there be a review process to ensure ongoing retention of the BPD was lawful.

57) Thus, in 2006, MI5 agreed and issued the policy document "Bulk External Data Acquisition - Internal Authorisation Process". This policy document was, initially, trialled (on 13 October 2006) in one part of the data analyst team but was then extended, on 6 November 2006, to the rest of the team. By late 2006/early 2007, the 2006 policy document was adopted across the Service generally. Thereafter, the policy and practice of MI5, in relation to the acquisition of BPD and review of BPD, followed this 2006 policy document over the period until the 2010 policy was adopted in October 2010.

58) I am told that the significant policy driver within the data analyst team in the period from 2006 onwards was to prioritise and focus the acquisition of BPD. Our analytical systems had (and still, to this day, have) a limited capacity to ingest BPDs and our people resource likewise meant (and mean) that we needed (and continue to need) to assess carefully whether there was/is a sufficient business need and justification before BPD is acquired or retained.

59) Thus, one of the changes instituted by the 2006 policy was the creation of the role of section data coordinator (mentioned in Annex B to the 2006 policy [page 183]). As well as being the key person, from that section, to participate in the review of whether or not retention of BPD was necessary and proportionate, that person's role was also to coordinate, ie prioritise, requests for acquisition from his/her section. That latter role was vital because we did not have the capacity to simply acquire every BPD that investigators/sections might wish for. Thus, and for business and operational reasons alone we had to focus – in our decision-making about acquisition of BPD - on those BPDs that we believed would be most valuable. The review process was another key way to ensure that we were only retaining BPD where there was a genuine need to do so. In particular, over the period from 2006 onwards, at every 6 monthly review of BPD, each of the BPDs then held by MI5 was reviewed.

Acquisition, sharing and retention forms

60) At items 4 and 5 of the "Historic disclosure" we have provided copies of early versions of MI5's bulk data acquisition authorisation forms. In the case of item 4 the form was an annex to the 2006 policy [pages 185-188]. At items 6, 7 and 8 of the "Historic disclosure" we have provided copies of various later versions of MI5's data acquisition forms [pages 191-216], as well as its sharing [pages 217-238] and retention [pages 239-264] forms.

61) Additionally, I am now able to produce and exhibit a further data sharing form (DSF V1) [pages 809-812] and four further data retention forms (DRF V1-V4 - [pages 787-802]). Further, during May 2016 we updated our form for data retention. The current version (DRF V8) is also produced [pages 803-808].

62) I am able to confirm that the various acquisition, sharing and retention forms disclosed and now produced and exhibited were first issued/used within MI5 on or about the following dates:

Acquisition forms:

- V3-0: July 2009
- V5-0: November 2010
- V7-0: June 2014
- V8-0: August 2015 (this being the current version in use)

Sharing forms:

- DSF V1: February 2011
- DSF V3.1: January 2012
- DSF V4: January 2014
- DSF V5: March 2015 (this being the current version in use)

Retention forms:

- DRF V1: February 2010
- DRF V2: July 2010
- DRF V3: January 2012
- DRF V4: January 2013
- DRF V5: May 2014;
- DRF V5.1: June 2014;
- DRF V 6: March 2015;
- DRF V6.2: May 2015;
- DRF V7.1: July 2015
- DRF V8: May 2016 (this being the current version in use).

63) The standard acquisition form (as annexed to the 2006 policy document [pages 185-188]), which was used from approximately late 2006/2007 onwards includes specific questions (and sub-questions) as to the necessity and proportionality of acquisition of BPD. As is apparent from the various acquisition forms at [pages 191-216], that has continued to be asked, and is the key question that has gone to the heart of all decision-making in relation to whether or not a BPD should be acquired.

64) As appears from acquisition form V7 [pages 205-206] (section 3 of the form) as from June 2014 (when this version of the form came into use) it became a requirement of the BPD acquisition process that a lawyer within MI5 complete a "Legality of Acquisition" section in the form confirming their view as to the legality of the proposed acquisition of the dataset.

65) MI5 shares BPD with GCHQ and SIS where this is in support of our statutory functions and where it is considered necessary and proportionate to do so. Were we to share with foreign partners, that would be on the same basis.

66) BPD that we acquire comes from a range of sources, including from GCHQ/SIS and other Government departments. Such BPD is always obtained with their knowledge and co-operation.

2010 Policy for Bulk Data Acquisition, Sharing, Retention & Deletion

67) MI5 issued the above policy, covering all aspects of the BPD process, in October 2010. The 2010 policy [pages 17-28] was thus intended to act as a description of the policy to be followed in relation to all aspects of our acquisition, access, retention and deletion of BPD. Additionally, the Annex was intended as internal guidance for investigators and managers. The 2010 policy was intended to further formalise and describe our processes for handling BPD, in particular following a Cabinet Office review in relation to the SIA's use of BPD, and at a time when the BPD regime was coming under the oversight of the Intelligence Services Commissioner.

68) The 2010 policy remained in force (subject to some changes, see further below) until it was replaced, in early 2015, by the SIA BPD policy at RF1 1 [pages 309-318]. I am told that our practice and process followed the 2010 policy (as amended, see further below) over this period. The SIA BPD policy was issued in February 2015 and became the overarching policy document as supplemented, internally for MI5 staff, by the BPD Guidance (issued in March 2015) which is at item 15 of the RFI disclosure [pages 35-46].

69) The 2010 policy, when issued in October 2010, specified a date for its review of October 2011. Although I am not able to point to a specific review of the policy having taken place in October 2011, I am told that the 2010 policy was kept under ongoing consideration, by the data governance team until it was replaced in early 2015. However, over that period there were three particular changes in policy/practice that I should mention. These changes were to:

a) The approach taken to datasets acquired from overt sources;
b) The review process adopted for BPD; and
c) The approach taken to datasets acquired through RIPA/ISA.

70) Firstly, there was a change in policy/approach that was agreed in late 2012. This was to bring within the BPD regime certain types of data that had, until then, been outside the regime. In particular:

a) The 2010 policy [page 18] (see the third paragraph) provides that: *"Finally, commercially and openly available datasets (e.g. GB info, Companies House etc) and data generated by corporate systems is not bulk data. The handling of these datasets is not covered by this policy."*

b) However, in late 2012, MI5 decided to treat commercially and openly available datasets as BPD and that approach was adopted, from then, as a matter of practice.

71) We changed our approach, deciding to treat these datasets as BPD because, upon further consideration of the nature of these types of datasets, we concluded that the fact that we had acquired these from overt sources did not mean that there was not a degree of interference with the privacy of those whose personal data was within these datasets. In particular, we concluded that the fact that the datasets were already in the public domain (and much of the personal data may indeed have been put there by the individuals concerned) should not be regarded as so significant a factor as to exclude these datasets from the BPD regime, in circumstances where MI5 was putting this data (relating to persons the majority of whom would not be of intelligence interest) on its analytical systems.

72) In relation to our review process for BPD, we modified the approach taken by the BPD Review Panel when reviewing BPD at their 6 monthly meetings. This modification was reflected and recorded in the October 2012 Bulk Data Retention and Deletion Policy (item 14 of RFI disclosure [pages 29-34]). In particular:

a) Although it remained a requirement that a retention form had to be completed for each BPD for each 6 monthly meeting of the BPD Review Panel (and the retention forms for every BPD would be reviewed by the data governance team) at the BPD Review Panel meetings, the Panel would not consider every BPD held.

b) Rather, as from October 2012 onwards, the Panel would review any new datasets acquired since the previous meeting, datasets giving rise to issues (eg lack of usage or held but not yet ingested) and any datasets not reviewed in the previous two years.

c) This change in relation to what was considered at BPD Review Panel meetings was a reflection of the fact that we had, since 2006, acquired an increasing number of datasets, such that reviewing each of them, every 6 months, was not practical and not considered to be necessary in order to address the ongoing need for retention.

73) There was some further modification of the review process, taken by the BPD Review Panel, in October 2014. In particular it was decided that the review periods for BPD should be determined by reference to: intrusion, corporate risk, usage and themes.

74) In particular, we concluded that intrusion and corporate risk should be the primary determinants of the review period for a particular BPD, such that:

a) high intrusion or corporate risk, would lead to a review every 6 months,

b) medium intrusion or corporate risk, would lead to a review every 12 months, and

c) low intrusion or corporate risk would lead to a review every 2 years.

75) Additionally, if there was low usage or some other concern raised, then a BPD would be referred to the Panel for discussion. Finally, the Panel may also review datasets by reference to themes. Themes discussed to date have been defined by geographical area and types of threat.

76) I have exhibited a copy of two Loose Minutes (dated 19 September 2014 [pages 813-818] and 21 October 2014 [819-820] that describe the October 2014 modification to the review process.

77) The third change in practice/policy in the period between 2010 and 2015 was in relation to bulk personal data acquired through a RIPA (or ISA) authorised process eg interception (or property/equipment interference). Under the 2010 policy we excluded from the BPD regime datasets acquired in this way. However, as from Autumn 2013 we concluded (as we had done in late 2012 in relation to BPD acquired from overt sources) that the means of acquisition ought not to exclude from being BPD a dataset that otherwise had the key characteristics of BPD. Thus, where applicable, parallel authorisation processes (a Secretary of State warrant for interception and a MI5 internal authorisation for acquisition of BPD) will be required where a BPD is sought to be acquired by interception.

MI5's BPDs are (and always have been) obtained, without using RIPA/ISA powers, from, and with the knowledge of: SIA partners, other Government Departments or public bodies and law enforcement partners.

78) Ongoing review of MI5's BPD policy and practice, over the period from 2010 to 2015, is also evidenced by the various iterations of the standard forms for the acquisition, sharing and retention of BPD over this time.

BPD policy and guidance since 2015

79) By 2014 MI5 had recognised the desirability of aligning our BPD policy approach with that of SIS and GCHQ and so, in conjunction with them, it was agreed to prepare a single policy framework across the three agencies. This resulted in the 2015 cross-SIA BPD policy of February 2015 at [pages 309-318]. This was supplemented by MI5 Bulk Personal Data Guidance dated March 2015 (item 15 of the RFI disclosure [pages 35-46]) which gave more detailed staff guidance.

80) The February 2015 SIA policy document was then updated in November 2015, as per item 17 of the RFI disclosure [pages 67-82]. Although that document has the date of February 2015, I can confirm that this was in fact updated in November 2015. On 4 November 2015 the SIA published the cross-agency handling arrangements for BPD.

81) In November 2015, MI5 also updated its internal BPD Guidance document in the form disclosed at item 16 of the RFI disclosure [pages 47-66]. That internal BPD guidance for staff now sits alongside the internal MI5 Handling Arrangements for BPD that were issued in November 2015 (item 21 of the RFI disclosure [pages 101-114]). I confirm that these internal MI5 Handling Arrangements set out and describe our current practice and procedure in relation to the acquisition, use, retention, review, deletion and oversight of BPD.

Statutory Codes of Practice

82) There is no statutory code of practice regulating BPD. However, depending on the means of acquisition of the BPD, one of the Codes of Practice issued under the Regulation of Investigatory Powers Act 2000 ("RIPA") may be relevant and applicable.

83) MI5's current Handling Arrangements (paragraphs 2.10 and 2.11 [page 103] recognise that in the event that, for example, RIPA or ISA statutory powers are used to acquire a BPD (say interception) then the applicable regime relating to those powers (including any applicable RIPA or ISA Code of Practice) will need to be complied with, and the requirements of the BPD Handling Arrangements will apply in addition to and/or in parallel to that statutory regime. Accordingly, if we wished to seek to obtain a BPD through interception, we would seek the necessary interception warrant from the Secretary of State and, in parallel to that, would follow our internal process for the acquisition of BPD.

Retention and Review periods

84) The BPD Handling Arrangements (item 21 of the RFI disclosure [pages 110-112]) describe the current review process. All new acquisitions will be subject to an initial review by the BPD Review Panel at the first meeting after acquisition. If a decision is taken to retain the dataset, then a review period of between 6 months and 24 months will be set, and continued retention will then be considered at the meeting after that period.

85) In determining whether to set a review period of 6, 12 or 24 months, the key factors that the Panel will consider are the level of intrusiveness of the dataset and the level of corporate risk. Retention forms are required in advance of the Review Panel meeting at which that BPD will be discussed. The approach I have described above of the BPD Review Panel discussing particular BPD where there may be concerns (eg of low usage), and of reviewing datasets by reference to themes, continues to apply.

86) I have referred, above, to the review periods for BPD, these being the dates/frequency with which MI5 decides whether to continue to keep/use (and, as appropriate, receive updates for) a dataset. That review period (of between 6 and 24 months) for the dataset is to be distinguished from the retention period for data, the latter being the date from which data will be deleted. Thus, at the end of the retention period, data of a certain age (within that dataset) will be scheduled for deletion (because it is not considered necessary and appropriate to continue to hold that data). However, we may still use/keep that dataset (using data within that dataset that is still within the retention period). If the Panel decides that it is no longer necessary and proportionate to hold all or part of a dataset, deletion will be triggered by that decision rather than the longer retention date.

87) The retention period for which MI5 holds BPD is sensitive because revealing the date when data will be deleted would enable persons to determine when individuals would no longer appear in datasets and thus, when particular people would be "off our radar" and might be capable of being used/deployed without appearing in searches conducted by us.

Secure systems where BPD is held

88) The vast majority of MI5's datasets are held on (and only on) our analytical systems and only staff who have signed the applicable MI5 internal Code of Practice (as disclosed at exhibit D to the CLOSED response [pages 305-308]) are able to access these. The Code of Practice has to be re-signed by staff on an annual basis. This Code is additional to a code of practice that all staff have to sign to have any access to the IT system and which requires all staff to confirm, every time they log onto the IT system, that they agree to and which reminds that

failure to comply with that code is a disciplinary offence and that their use of the system may be monitored.

89) The Code at exhibit D makes clear to staff the particular restrictions that apply to their access to the analytical systems area and explains the rationale for this. It advises staff that their activities will be monitored and that misuse of the system may result in disciplinary action. The Code spells out in unambiguous terms that they may only use the analytical systems for legitimate business reasons and that access is authorised only where there is a legitimate purpose (relating to the functions of each person's job) and where the individual is satisfied that using the analytical systems is necessary and proportionate.

90) Access to the BPDs stored outside the analytical areas is restricted to those with a specific business need. Anyone accessing the non-analytical areas will have had to sign the code of practice that all staff have to sign to have any access to the IT system.

91) When authorisation to acquire a dataset is in process, one of the matters that is considered is whether or not there are any particular restrictions that ought to be applied to ensure that that dataset is only available to particular persons or specialist analysts within MI5. I refer, in this regard, to section 2 of the current standard form for acquisition (item 18 of the RFI disclosure [page 84]) and the rows relating to proposed destination systems and proposed access restrictions.

92) Criteria which will inform decision-making as to the system onto which the dataset will be loaded will include: whether there is any particular sensitivity in relation to the data or the source of the dataset, and whether it is necessary for the data to be made available to all investigators.

<u>Training</u>

93) In order to access the analytical systems where the vast majority of BPD is held, as well as signing the Code of Practice [pages 305-308], staff must also have completed training relevant to the analytical systems.

94) In the training, staff are told that they must:

a) ensure that they comply with the Code of Practice;
b) ensure that their activity on the systems is necessary and proportionate to their work;
c) not share raw data with persons not themselves authorised to access it;
d) report any accidental viewing of, or searching on, sensitive data; and to raise any concerns about use of the systems.

95) Additionally, staff are told that prohibited activities include searching out of their business area without a legitimate need to do so. Trainers will emphasise that use of the analytical systems is heavily audited and that staff may be subject to spot checks. Staff are asked, in terms, whether they read the Code of Practice before signing it, and are told it is important that they know what they have signed up to. They are told that they must ensure that their activities are necessary and proportionate and that they will need to be able to justify this, if questioned.

96) Intelligence officers within MI5 all undergo compulsory training when they join the Service. In their 2nd week (typically) of their induction training (after having joined the Service) intelligence officers will attend a two day course as part of the intelligence officer development training programme. Part of that two day course involves a specific session on the principles of necessity and proportionality. The training session also involves two group exercises where issues of necessity, proportionality, justification and intrusiveness are discussed and considered.

97) I have referred above, to the specialist analysts and that some of the MI5 BPD are only made available to these specialist analysts. The specialist analysts work alongside investigative teams and provide support to investigators. They will, typically, work on the more complex cases and will be able to search across the analytical systems generally, but also the particular sections of these that others will not have access to.

98) These specialist analysts receive particular training on necessity and proportionality. This training gives detailed guidance, by reference to examples and scenarios, as to how necessity and proportionality should be assessed when carrying out analysis of BPD and also explains how necessity and proportionality is considered when the acquisition of BPDs is determined.

Independent oversight

99) MI5 keeps the Home Secretary appraised, on an annual basis, of its BPD holdings and key matters in relation to its policy relating to, and use of, BPD. In particular, we provide to the Home Secretary a full list of our BPD holdings each year and have done so since 2012.

100) Since 14 October 2010 the Intelligence Services Commissioner has had formal oversight of MI5's acquisition and use of BPD. The Commissioner has exercised oversight of BPD throughout the period since October 2010. On a twice yearly basis we have provided to the Commissioner a full list of all BPD then currently held by us. The Commissioner will, typically, select particular BPD for detailed review and ask us specific questions about these. We provide answers to such questions, and make available to him such information as he may require.

Where, on occasions (see further below), we have not followed due process in relation to BPD, we report that to the Commissioner.

101) Since 11 March 2015, and the Prime Minister's direction on that date, the Intelligence Services Commissioner has had statutory oversight of MI5's use, retention, and disclosure of BPD, and of the adequacy of safeguards against misuse.

102) The Intelligence and Security Committee was given formal notification of MI5's use of BPD in March 2014.

Instances of misuse of BPD

103) Access to BPD through the analytical systems (where, as mentioned above, the vast majority of all BPD is kept) will always result in the creation of an audit log, which enables a range of audit measures to be undertaken. The monitoring of access to BPD is prioritised within the monitoring team, using a range of security alerts or any other information which the monitoring team may have been provided with which might indicate misuse of BPD. This would then be investigated further depending upon an assessment of the potential risk.

104) I confirm that I have seen the Reply to the Request for Further Information dated 30 March 2016. Whilst, of course, any single instance of non-compliance with our procedures/policies is a matter of concern, it is important that these instances were identified, reported and looked into.

Proportionality

105) Whilst it is right to acknowledge that simply holding personal data relating to individuals, who are not of intelligence interest, does give rise to privacy implications; the extent of privacy interference is, I suggest, minimal. The personal data of the vast majority of persons on a BPD will never, in fact, be seen, read or considered by MI5 because it will never feature as a search result.

106) Further, it is important to state that when considering acquisition of a BPD, we will consider if particular fields of data within a BPD do, or do not, need to be acquired. If not necessary, then there is the potential for us to ensure that such fields are not provided to us, or that we do not ingest such fields, when loading the dataset onto our analytical systems.

107) BPD is important not just because it is as an investigative tool that is quick and effective, but also because it reduces the degree of collateral intrusion that might otherwise be required as part of a legitimate investigation.

108) By way of example, in relation to a suspected Al-Qaeda operative who was believed to be facilitating suicide bombers in the UK, the intelligence agencies had a general description, but no name. Contact information received did not immediately identify the individual. However, analysts with access to BPD were able to identify possible matches and quickly narrow this down to one strong match. At that point, there was a sufficient case to justify more intrusive methods to cross-check the information. Had it not been possible to use BPD to narrow the investigation down to one strong person, then it would have been necessary to investigate a wider range of individuals in a more intrusive manner.

SECTION 3 – BULK COMMUNICATIONS DATA

Background

109) The first directions, at the instance of MI5, to communication network providers for the provision of BCD were issued in July 2005. I note that in some of the documents, including the correspondence (referred to below) with Sir Swinton Thomas, the terms communications service providers ("CSP") is used. For the sake of consistency, I use the term CSP in this document.

110) Consideration as to the acquisition of BCD had begun in MI5 during 2003, and by early 2004 MI5's Director General had formed the view that, in order to counter the threat from international terrorism ("ICT"), MI5 needed to have access to a BCD database. Communications data ("CD") had proved itself as invaluable in ICT investigations but MI5's ability to use CD as effectively and quickly as was needed was constrained by the fact that the data was not held by MI5. In particular, it was recognised that, in complex and fast-moving investigations, having access to a database of BCD would enable MI5 to carry out more sophisticated and timely analysis, by joining the dots in a manner that would not be possible through individual CD requests made to CSPs.

111) The Respondents have disclosed, for the purposes of this claim, correspondence in 2004 between the Home Office and Sir Swinton Thomas (then the Interception of Communications Commissioner) referring to the consideration being given, at that time, to the acquisition of BCD [page 821-831]. As can be seen from this correspondence, the view of the Home Office legal advisers was that the appropriate means of acquisition of BCD was through a section 94 direction, rather than use of Part 1 Chapter II RIPA.

112) It is my understanding that the two key reasons for using section 94 are those put forward by the Home Office legal advisers at paragraphs 4 and 5 of their letter to Sir Swinton Thomas of 22 June 2004. Those were:

a) That the decision as to whether or not to acquire the data would be that of the Home Secretary, not that of a member of staff of MI5. As the letter points out, even allowing for the possibility of escalating to a senior level at MI5, the decision as to acquisition, if the BCD were to be acquired under RIPA powers, would still always be by an official.

b) The recognition that CSPs were concerned that, if the acquisition of BCD was at the instance of MI5 not Ministers using RIPA, this may lead to other public authorities, for law enforcement purposes, setting up a bulk database. Section 94 directions can, of course, only be used where that is necessary in the interests of national security.

113) The use of section 94, to authorise the acquisition, with the consequent need for the Home Secretary's agreement not only to the issuing but also the continuance of the directions meant that the necessity and proportionality decision, on what is obviously a capability of some significance, was thus taken not by MI5 (even at the highest level here) but by a Secretary of State.

Setting up the database

114) Following the issuing of the directions in July 2005, it was necessary to undertake work to establish the database and ensure that it functioned as it should. That work was completed by May 2006 when the database became functional in that, for the first time, it could be used to obtain CD.

115) The database was initially operated, internally within MI5, as a pilot project. Over the following months there was regular assessment of the functioning of the database and in particular of the compliance regime for it. In October 2006, the view of those assessing the pilot was that the process for authorising and searching the database (namely following the RIPA Part 1 Chapter II process) was well understood. Accordingly, in October 2006 the Deputy Director General of MI5 agreed to approve the pilot as an operational capability.

Safeguards

Acquisition

116) I deal, firstly, with the acquisition by MI5 of BCD from communication network providers (CSPs). The first, and perhaps most obvious safeguard that exists, in relation to MI5's ability to acquire BCD is that the independent view of the Home Secretary is required, both for the issuing of the original directions and for them to continue in force.

117) Successive Home Secretaries have approved the continuance of the section 94 directions.

a) In the period prior to September 2009 our records are not complete. However, I am told that updates/briefings in relation to the database were provided to the Home Office in the period 2006 to 2008 at least annually.

b) Since September 2009 MI5 has written to the Home Office, twice a year, providing our assessment as to the need for the database and seeking the Home Secretary's agreement to its continued operation.

Use and Access

118) MI5's database of BCD is held securely and the database is updated securely. The database is held separately from all our other data and it is not technically possible to combine/fuse the database with our BPD datasets or any other parts of our data holdings. Additionally, access to the database is further controlled in the manner described below.

119) As the 2004 correspondence with Sir Swinton Thomas makes clear, from the outset it was proposed that the means of regulating MI5's access to the database would be through MI5 following the same process, for requests of the database, as applied for CD requests to CSPs, namely a regime of authorisation, by a designated person, that would follow the Part 1 Chapter II RIPA process.

120) Prior to the database becoming functional (in May 2006), the Loose Minute of 31 March 2006 (item 9 of the Historic disclosure [pages 265-266]) provided clear guidance and explanation that the system for authorisation of access to the database would be the RIPA Part 1 Chapter II process. This is the authorisation regime that has applied to all requests for CD that have been made of the database from its inception up to the present day. At items 10 to 15 of the Historic disclosure [pages 267-278], MI5 has provided further notes/minutes relating to the requirements that needed to be met for authorisation to be given for access to the database.

121) Access to the data in the database is controlled - technically - in such a way that requests of the database can only take effect if an authorisation is granted through the electronic system for processing CD requests. Accordingly, although our internal CD guidance (see further below) also refers to the possible use of forms for the making of CD requests, access to the database would additionally require processing a request (dealt with on paper) on the electronic system.

122) The electronic authorisation process that we have used to enable requests to be made of the database has been in place from when the database was first commissioned and used in May 2006 and is the same electronic system as is used for all CD requests that require CSP action. Thus, an investigator or analyst will always need to use MI5's electronic system for the processing of CD requests, whether that CD request is then answered by interrogation of the database of BCD or whether that request is then forwarded to the CSP.

123) All CD requests (whether through the electronic system or on paper) require a necessity and proportionality justification. As part of the disclosure exercise undertaken for the purposes of this claim, MI5 has disclosed versions of its internal guidance for staff (as have been in force from February 2011 to the present date) in relation to how to address necessity and proportionality when making CD requests and to enable Designated Persons to identify justifications which are incomplete. As at February 2011 necessity, proportionality and collateral intrusion questions were covered in one box on the electronic system. However, since January 2012 three separate boxes on the electronic system for the processing of CD requests have had to be completed to cover these matters.

124) I am told that the dates of issue of these guidance documents (issued by the warrantry team and which have all been published on the internal MI5 intranet) are as follows:

- Item 16 of the Historic disclosure [pages 279-284]: issued in February 2011.
- Item 17 of the Historic disclosure [pages 285-290]: issued in January 2012.
- Item 18 of the Historic disclosure [pages 291-298]: issued in April 2012.
- Item 19 of the Historic disclosure [pages 299-304]: issued in December 2012.
- Item 22 of the RFI disclosure [pages 115-118]: issued in November 2013.
- Item 23 of the RFI disclosure [pages 119-124]: issued in January 2015.
- Item 24 of the RFI disclosure [pages 125-132]: issued in October 2015.
- Item 25 of the RFI disclosure [pages 133-142]: issued in November 2015.
- Item 26 of the RFI disclosure [pages 143-152]: issued in March 2016 and current.

125) As well as providing guidance to those completing CD requests, the guidance also provides advice for designated persons as to the matters that they must consider when assessing CD requests. The guidance in force between February 2011 and January 2012 (item 16 [pages 279-284]) specifically set out the following in relation to (i) Necessity; (ii) Proportionality - General; and (iii) Proportionality - Collateral Intrusion:

a) Necessity:

"Necessity can be divided into three main points that need to be considered in any communications data justification:

- Background to the investigation - what is it that we are investigating?

- What is the subject of the communication data request's relation to the investigation?

- How does the communications address that we are making the request for relate to the target and to the investigation?

The applicant must be able to link these three points together in order to demonstrate that any request for communications data is necessary for the statutory purpose specified."

b) Proportionality:

"When considering proportionality, applicants need to outline how obtaining the data will benefit the investigation and what intrusion into privacy the request will result in. The main things that need to be considered are:

- What are you looking for in the data to be acquired?

- If the data contains what you are looking for, how will this assist you in taking the investigation forward?

- What will be the intrusion into the privacy of the target of the request? Will there be any other intended intrusion taking place?

- Is there another, less intrusive way of obtaining the information you need?

- If a time period of data has been specified, why is this particular time period required e.g. why would a shorter time period not be sufficient?

Therefore, the applicant should explain how the communications data will be used once obtained and how this will benefit the investigation. It is also important that intrusion into the target of the request's privacy is considered.

These points form a large part of the proportionality argument, the other part being in relation to collateral intrusion."

c) Proportionality - Collateral Intrusion:

"As mentioned above, collateral intrusion forms part of the proportionality argument.

The key question to be asked in relation to this is:

– Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for? How will this be mitigated?

– If a time period of data has been specified, how will this impact on the identified collateral intrusion?

When considering this question, the applicant should not detail potential or hypothetical errors. [REDACTION]

Therefore, collateral intrusion should always be considered and described if it is identified. However, it may be that none can be identified. When this is the case, then this should be stated. For example, telephone subscriber checks are unlikely to result in any collateral intrusion."

126) In addition guidance was provided for Designated Persons requiring them to *"take care to scrutinise"* applications for communications data, *"particularly the justification page"* before authorising them. Key points to be checked by the Designated Person were:

"- Taking into account the guidance for applicants above, that the justification provided by the applicant is sufficient to satisfy the DP that obtaining the requested data is both necessary and proportionate

– That the individual mentioned in the justification is identical with the one for which the data is being obtained, that is that the justification has not been "copied and pasted" from another application

– That the intrusion into privacy that will result from the request has been addressed where necessary and where identified, measures to mitigate collateral intrusion have been outlined

- That the time period of data requested is proportionate and that the reasoning for requesting the time period listed is explained in the justification"

127) Designated Persons were *"required to reject any application for communications data where they are not convinced of both the necessity and proportionality of the request".*

128) Subsequent versions of this guidance were essentially identical, albeit with some minor changes of phrasing, and save that:

a) From January 2012 (Item 17 of the RFI disclosure [pages 285-290]) onwards the guidance explained the National Priority Grading System (NPGS) detailed in the Communications Data Code of Practice;, which categorised requests for communications data as Very Urgent, Urgent and Routine.

b) From November 2013 (Item 22 of the RFI disclosure [pages 115-118]) onwards more guidance was given as to the term "meaningful collateral intrusion":

" "Meaningful collateral intrusion" includes collateral intrusion that we can foresee is "highly likely" – such as family members using the landline or internet connection where they live. However, we should not speculate where possible collateral intrusion cannot be said to be "highly likely"..."

c) From November 2015 (Item 25 of the RFI disclosure [pages 133-142]) onwards:

i) Specific attention was drawn (and a link provided to) to the MI5 Section 94 Handling Arrangements which came into force on 4 November 2015; and

ii) Detailed guidance was provided in respect of communications data applications relating to members of sensitive professions.

129) I am also able to confirm, based on what I have been told, the dates of the following additional documents that were disclosed in the RFI disclosure for the period 2014-2015 and which relate to the regime and process for consideration of CD requests:

- Item 27 [pages 153-154]: issued in September 2011.
- Item 28 [pages 155-156]: issued in August 2014 and current.
- Item 29 [pages 157-158]: issued in April 2015 and current.
- Item 30 [pages 159-160]: issued in April 2015 and current.
- Item 31 [pages 161-162]: issued in October 2015.
- Item 32 [pages 163-176]: issued in November 2015 and current.

Retention period

130) BCD in the database is currently retained for 1 year. When the database was initially set up the anticipated retention period for the data was 6 months, but in approximately 2007 the period of retention was extended. For some periods in 2007-2008 the database held data for a period of between 12 months and

approximately 18 months. However, since December 2008, the database has not held data that is more than 365 days old. Since November 2009, the database has held data for 365 days (automatically deleting any data that is older than 365 days).

Codes of Practice

131) The authorisation process for access to the database was from the outset, as described above, the same as for requests to CSPs for CD under Part 1 Chapter II of RIPA, and as a matter of practice and policy, MI5 has applied the applicable Codes of Conduct for the acquisition of communications data to the regime that it has operated for access to the database. In particular, investigators would – when completing requests for CD – be expected to comply with applicable parts of the Code of Practice relating to the acquisition of CD.

Handling Arrangements for BCD

132) In November 2015 MI5 issued the handling arrangements for BCD as disclosed in a redacted form at item 32 of the RFI disclosure [pages 163-176]. I confirm that – save in the respects mentioned below at paragraphs 143 to 149 - these set out and describe our current practice and procedure in relation to the acquisition, use, retention, review, deletion and oversight of BCD.

Sharing

133) Strict controls exist in our Handling Arrangements relating to the sharing of the BCD database or a subset of it. This would necessitate the approval, internally, of the Director General and external agreement from the Home Office.

Training

134) I have mentioned above, in the context of BPD, the training that all investigators currently receive in relation to necessity and proportionality. The guidance to investigators and designated persons, referred to above, provides ongoing training and support in relation to their obligations in relation to making requests for CD.

Independent oversight

135) From the outset of MI5's proposed use of section 94 to acquire BCD we recognised the importance of oversight not just by the Home Secretary, who would be regularly reviewing the directions, but also that of the Interception of Communications Commissioner.

136) The database became operational in May 2006 and, following the pilot phase, became fully adopted in October 2006. Sir Swinton Thomas had been aware of the proposal to establish the database from 2004, but by 2006 Sir Paul Kennedy had taken over as the Interception of Communications Commissioner.

137) Sir Paul was briefed in relation to the database in November 2006 and conducted his first review of MI5's access to the database as part of his next inspection in June 2007. Sir Paul continued to exercise oversight of our access to the database throughout his time as Interception of Communications Commissioner (up to late 2012) reviewing paperwork in relation to access to the database at each of his 6 monthly inspections and being informed of reportable errors in relation to access.

138) Sir Anthony May was briefed in relation to the database at his first inspection, after his appointment as Interception of Communications Commissioner, in May 2013. As with his predecessor, where reportable errors have occurred in relation to our access to the database, we have reported these to the Commissioner.

139) In January 2015 the Prime Minister asked Sir Anthony May (in his role as Interception of Communications Commissioner) to extend his oversight of MI5's database capability. In particular, it was agreed that Sir Anthony May's oversight would be extended to cover the issuing, by the Secretary of State, of the section 94 directions and of our retention, storage and destruction arrangements for the data.

140) On 4 November 2015 Sir Stanley Burnton was appointed as Interception of Communications Commissioner. He was given an initial briefing in relation to the database on 15 December 2015 and was provided with further explanation on 18 May 2016.

Instances of non-compliance in relation to section 94 BCD

141) In the Reply to the Request for Further Information dated 30 March 2016 we have provided details of instances of non-compliance (in the period from June 2014 to February 2015) in relation to MI5's access to the database.

142) Those figures include instances of errors where no data will have been received, because the error in the request was noticed (eg by the designated person) before the request for CD was approved. Such errors are recordable, and we have considered to be examples of "non-compliance" albeit that they would not be "reportable" to the Interception of Communications Commissioner. A reportable error occurs where the error results in CD being acquired (or wrongly disclosed).

143) In relation to the errors relating to MI5's use of section 94 BCD, as referred to in the Response of 30 March, I am told that:

a) Three of the four errors noted at (a)(i) were reportable (and have been reported to the Commissioner); and
b) 20 of the 43 errors noted at (a)(ii) were reportable (and have been reported to the Commissioner).

Additional instances of non-compliance

144) Since serving the Response to the Request for Further Information, we have become aware of some additional instances of non-compliance. These relate to the regime for accessing the database.

145) Paragraphs 4.3.4 and 4.3.5 of the Handling Arrangements for BCD [pages 168-169], and the RIPA process that we have followed for regulating access to the database, require an applicant, before submitting a request for authorisation, to include in the request the considerations relating to necessity and proportionality. There must, accordingly, exist (when a request is made and before it is authorised) a written record (whether on paper or electronically) of the necessity and proportionality justification for the request being made.

146) We have identified that a proportion of requests of the database have been authorised without a written record of the necessity and proportionality case for obtaining the required data being made in advance. Rather, in these instances, the necessity and proportionality case was made by the applicant orally to the designated person and agreed by the designated person orally, with the request then being submitted on the electronic system, and then being authorised.

147) In these cases, the record of the necessity and proportionality case has either been written up retrospectively (sometimes after a number of days or, on occasions, weeks), or in some cases, has not been written up (prior to this non-compliance issue having been identified).

148) Additionally, we have identified some instances where written justifications were not completed prior to oral authorisation of the request and then authorisation on the electronic system. In a very small number of cases there is no record of written authorisation.

149) This non-compliance issue was discovered on 3 May 2016, having been identified by someone who had recently started as a designated person (authorising requests for access to the database). On 4 May we issued a reminder to relevant designated persons of the requirement for there to be a written record

of the necessity and proportionality for each request before a request can be authorised.

150) This matter was formally reported to the Interception of Communications Commissioner on 20 May 2016 (having been informally mentioned to him on 18 May 2016) and we are currently liaising with his Office in relation to their enquiries into this matter. Our investigation into this matter has looked at the period since 1 November 2010.

151) I will provide a supplementary witness statement, as soon as is practicable, in order to give further details as to the nature and extent of the non-compliance with the regime for accessing the database and to describe the steps we have taken/will be taking, to avoid any recurrence.

Proportionality

152) In my capacity as Deputy Director for Data Access and Policy I saw how vital BCD is for the work of MI5, in particular in relation to counter-terrorism work. I am able to say, based on what I have seen myself and been told by colleagues in MI5, that the use of BCD by MI5 has stopped terrorist attacks and has saved lives many times.

153) The acquisition of BCD enables MI5 to identify threats and investigate in ways that, without this capability, would be either impossible or considerably slower. In many case, communications data may be the only investigative lead that we have to work from. Further, without BCD, it would be necessary to carry out other and more intrusive enquiries; for example many more individual requests for CD or use other more intrusive powers in order to narrow the scope of a search. The inability to use BCD would therefore involve greater intrusion into the privacy of individuals.

154) I recognise of course that, simply by holding BCD that relates to individuals who are not of intelligence interest, and as with BPD, there is a degree of interference with the privacy of such individuals. However, the BCD in the database is, itself, anonymous. Further, and as with all bulk capabilities, whilst it is right to acknowledge that a significant quantity of information can be collected, only a tiny proportion of the data is ever examined.

Statement of Truth

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

MI5 WITNESS

.....MI5 Witness.....

Dated: 11/7/16

*Gists are underlined
Amendments are double-underlined

Witness: SIS Witness
Party: 5th Respondent
Number: 1
Exhibit: SIS exhibit
Date: 8.7.16

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

AMENDED WITNESS STATEMENT OF SIS WITNESS

---

1. I, SIS witness, of the Secret Intelligence Service (SIS), Vauxhall Cross, London, SE1, will say as follows:

2. I have been a member of the senior leadership since 2012 and in my current role, I oversee the compliance of SIS operations with the law and other relevant guidance and directives. I was Project Executive for the project to upgrade SIS's database analysis tool to its current version. In that content, I attend the six monthly meetings of the Data Retention Review Board.

3. I am authorised to make this witness statement on behalf of SIS. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within SIS.

4. Attached to this statement, and marked 'SIS exhibit' is a bundle of relevant documents. Save where otherwise stated, page numbers below refer to that exhibit.

5. This statement addresses SIS's use of, and the safeguards which apply to, Bulk Personal Datasets ("BPD"). For the avoidance of doubt, SIS does not use section 94 of the TA 1984 to acquire Bulk Communications Data.

6. I have read the statement prepared on behalf of the Security Service, and in particular the section which addresses the current national security threat in the United Kingdom. I agree with what is said in that section, and do not address the national security threat further in this statement.

BACKGROUND

DEVELOPMENT OF THE USE OF BULK PERSONAL DATA

7. Early bulk personal data exploitation efforts focused on SIS's corporate stores of information and linking records on subjects of interest. Early efforts also involved working with SIA partners to share information on subjects of interest where appropriate.

8. In the wake of the 7/7 bombings, the scale of the counter-terrorism (CT) threat to the UK became clear. The new CT targets were, in most respects, ordinary people with little or no readily identifiable profile. They did not necessarily have traceable intelligence careers or links with criminal enterprises. Information on terrorist identities and activities was hidden in amongst the large databases that capture records of all of society. Systems for holding data were small-scale, dispersed, often standalone and limited in functionality. Access was available to small numbers of users on a case-by-case basis. Aggregation of data and inter-connectivity between datasets was consequently limited. In short, early initiatives to exploit data were naturally limited by the technology available.

9. Numbers of bulk personal datasets and users grew and data became an increasingly important and impactful capability in the CT sphere. There was a gradual realisation of the potential of the capability and a corresponding appreciation of the surrounding legal and policy issues. As risks and issues were identified and understood, appropriate safeguards were applied.

BULK PERSONAL DATASET HOLDINGS

10. The number of BPD sets, the quantity and categories of data held fluctuates over time, and in accordance with current operational priorities for intelligence collection. Where it is no longer necessary and proportionate to retain data, it is deleted.

11. At present, SIS holdings fall broadly into four categories: biographical, communications, financial and travel.

12. A statement has been made by the Claimants in relation to medical data. I refer to the statement made by the Minister John Hayes on 26 April 2016:

"I am prepared in this specific instance to confirm that the security and intelligence agencies do not hold a bulk personal dataset of medical records. Furthermore, I cannot currently conceive of a situation where, for example, obtaining all NHS records would be either necessary or proportionate."

SIS can confirm that it does not currently hold, and has never held, a bulk personal dataset of medical records, whether sourced from UK or overseas healthcare providers, including the NHS. Occasionally, information which relates to health or medical conditions will appear in bulk personal datasets, for example the requirement for a braille passport.

13. Data comes from a variety of sources, including SIA and OGD partners. Where we have acquired data from OGD partners, it has always been with their knowledge and co-operation.

14. SIS does not categorise bulk personal datasets according to their sensitivity. Rather, each dataset is assessed as part of the acquisition and authorisation process to establish the format and content of the data. The assessment establishes the presence of any of the categories of data that SIS deems to be particularly sensitive. These categories are drawn from the Data Protection Act and the RIPA Codes of Practice and are: religion, political opinions, racial/ethnic origin, disability/medical condition, sexual orientation, financial, criminal activity, legally privileged information, journalistic source information, medical information and spiritual counselling. The presence of any such data is recorded in the assessment for each dataset. If there is no necessity and proportionality case to retain the data it is deleted. If the data is to be retained, the authorisation records a specific justification for keeping it.

15. As part of the authorisation process, each bulk personal dataset is rated high, medium or low for actual and collateral intrusion. There is detailed guidance for analysts who provide these evaluations (see SIS exhibit 5-12 and 13-20). All authorisations are reviewed by managers within the Data Directorate and are authorised by a senior official and a member of the legal team, placed on the corporate record and are available to the Intelligence Services Commissioner.

16. Also as part of the authorisation process, each bulk personal dataset is rated high, medium or low for risk. This is the risk to SIS were it to become known that the organisation holds the data (and not the operational risk of acquiring it which is recorded in the relevant operational paperwork). This guidance for analysts is also detailed in SIS exhibit pages 5-12 and 13-20.

PROPORTIONALITY

17. The exploitation of bulk personal data is an essential tool for SIS in carrying out its statutory functions. Data is critical to the way SIS carries out, and defends, its operations. It is a critical capability that underpins our ability to respond to threats to the UK. The exploitation of BPD allows SIS to deploy resources proportionately where they are most needed by helping to eliminate the many who are not of interest to our operations and focus on finding the needle in the haystack.

18. SIS only acquires and retains bulk personal datasets where it is deemed necessary and proportionate for the purposes of carrying out its statutory functions. Once authorised and available in analytical tools, every search of BPD is required to have a justification and must be linked to a specific investigation. The necessity and proportionality of each search must be individually justified. All such justifications are recorded and audited, and subject to oversight. The vast majority of records will never be accessed or viewed.

19. We share data with our domestic partners in support of our statutory functions, where it is considered necessary and proportionate to do so. Were we to share with foreign partners, it would be on the same basis.

20. Systems for accessing bulk personal data are designed to limit actual and collateral intrusion as far as possible. In addition, staff are directed to construct their searches to limit collateral intrusion as far as possible. As a result, most of the data in the database will never be hit on as a result of a search.

21. Particular examples of the benefits of BPD include the following:

    Intelligence indicated that a partially identified associate of a known subject of interest aspired to travel to Syria for extremist purposes. Using BPD, agency analysts were quickly able to identify the associate, enabling rapid focus of investigative effort on the one individual of concern and discounting hundreds of other potential candidates. Without access to BPD, a resource intensive and more intrusive process would have been needed to identify the individual from the hundreds of potential candidates, incurring collateral intrusion into individuals of no intelligence interest and with significant risk of failing to identify the individual prior to travel.

22. Whenever bulk data is exploited SIS must always first consider the proportionality of carrying out the search, this includes consideration of whether any less intrusive means could be used to achieving the same objective. This means that in some cases all other means of achieving the same result (if any exist) will have been exhausted; in other cases, as set out in the example above, the alternative process would have been both more resource intensive and more intrusive, for example involving the use of legal intercept or surveillance.

SAFEGUARDS

OVERVIEW OF SAFEGUARDS SINCE JUNE 2005

23. The power for the Service to obtain information is provided for in the Intelligence Services Act 1994 ("the Act"). Since the introduction of the Act, SIS staff have been educated on the provisions of the Act and their responsibilities in regard to it at induction, on relevant internal training courses and in official documentation.

24. SIS applies, and has applied since the relevant time, the appropriate Home Office Codes of Practice when exercising their statutory powers and duties. Therefore, where any BPD is acquired using a statutory power to which a Code of Practice applies (e.g. under RIPA 2000/ISA 1994), then the provisions of the relevant Code will apply to the acquisition of that dataset or part.

25. Bulk personal dataset acquisitions that carry a particular political or diplomatic risk or are otherwise sensitive are subject to particular legal scrutiny and may be the subject of a submission to the Foreign Secretary. This was the case pre-2005 and continues to date. During the summer of 2007, SIS conducted an internal review of the legal and management issues associated with data exploitation. It recommended that the justification for acquiring all datasets (not just those acquired covertly and submitted to the Foreign Secretary) should be recorded. An internal dataset authorisation process was established to record the necessity and proportionality of each acquisition. This has been in place since at least October 2007. The same review recommended the institution of regular data retention reviews, in line with practice at MI5.

26. In October 2008, the Board agreed to create a central team for managing knowledge and information. The first senior manager in charge of this team was appointed in December 2008. During 2009, SIS rolled out an analytical tool (the database) for holding all bulk data for members of staff who could demonstrate a business case for access to the system. In October 2009, a bulk data policy was published (see SIS exhibit 79-84) and this policy was updated in November 2010 (see SIS exhibit pages 49-54).

27. In early 2015, a joint SIA BPD policy was agreed (see SIS exhibit pages 121-130). This codified existing practice at SIS. In October 2015, an updated review and retention policy was agreed by the internal information policy group which assigned datasets to a review period based on their level of intrusion. This policy is detailed in SIS exhibit pages 131-134. The most intrusive bulk personal datasets are reviewed most often. The policy was discussed with the Intelligence Services Commissioner at his visit in November 2015. He noted that our practice matched that of MI5 and approved of our emphasis on intrusion as the primary consideration of review periods. As part of the policy development work on review and retention the legal

team agreed an updated guidance document for staff who assess the intrusiveness of datasets (see SIS exhibit pages 13-20). This has subsequently been issued to all relevant staff. SIS Handling Arrangements were published in November 2015 which codified existing policies and procedures (see SIS exhibit pages 65-78).

AUTHORISATION

28. As detailed in paragraph 25 above, SIS developed a bulk personal dataset authorisation process following a review in summer 2007. Prior to this date, some datasets would have been the subject of a submission to the Foreign Secretary and where applicable, the relevant Home Office Code of Practice would have been followed. The first authorisation form (see SIS exhibit pages 91-92) was used from October 2007 to February 2012 and was based on the one in use at MI5. It included a definition of *"bulk data"* as *"electronic information on multiple individuals or organisations containing untargeted individuals and sought or processed for intelligence purposes."* It required a description of the data, the system that it would be stored in and any particular access controls. It established a data-owning officer or team for the data and recorded proposed retention and review periods. It required a consideration of necessity and proportionality, including, but not restricted to whether the benefits of using the BPD could *"be achieved by other means without the use of bulk data"*, an explanation of *"the level of intrusion into privacy"* and whether *"the database contain[ed] a high/low proportion of people of no intelligence interest"*. The form was authorised by a senior officer. Consideration by a member of the legal team was sought if the dataset was felt to raise particular questions around e.g. intrusion, including specifically whether *"the data includes large numbers of people of no intelligence interest or is extremely intrusive/delicate e.g. medical records"*. Forms in SIS are circulated via an internal workflow system enabling officers to collaborate on a document.

29. The second version of the form which was in use between March and December 2012 (see SIS exhibit pages 93-96) included a statement clarifying when an authorisation was required and was an early attempt to define the scope of what we now know as bulk personal data. Contrary to the statement on the form, which did not reflect practice at the time, SIS confirm that this authorisation form was used for the acquisition and retention of all BPDs however acquired, including where it was acquired under an existing oversight mechanism e.g. RIPA. New sections were incorporated for recording the presence of any personal data or data on UK nationals or minors. In addition to the section on necessity and proportionality, a new section was incorporated specifically requiring an assessment of actual and collateral intrusion. The acquisition officer was required to sign and date and alongside the formal approval of a senior officer, and sign-off by a member of the legal team, confirming that holding the data complied with ISA 1994, DPA 1998 and the Human Rights Act 1998, was mandatory.

30. The third version of the form which was in use between January and December 2013 (see SIS exhibit pages 97-100) removed the reference excluding BPD acquired under existing oversight mechanisms, reflecting the ongoing practice. The form included a more detailed section on data intrusiveness to be completed by a member of the data transformation team following an assessment of the data. This recorded the presence of any data relating to protected characteristics or confidential information.

31. The fourth version of the form, which was in use between January 2014 and October 2015, was headed 'Authorisation of Bulk Personal Dataset' (see SIS exhibit pages 21-26) and included a definition of the term for the first time. In this form, there are tick boxes for recording the presence of any categories of data that SIS deem to be particularly intrusive. If the assessment has identified any such information and any of the boxes are ticked, the analyst is required to make a specific justification for retaining and exploiting this data. This version of the form included standard text for the legal section to elucidate the relevant considerations. In September 2015, a legal annex was appended to each new authorisation which set out the legal considerations in respect of the authorisation of BPD.

32. The fifth version of the form, which has been in force since October 2015 (see SIS exhibit pages 27-32), made minor amendments to the intrusiveness section to clarify the likelihood of the presence of intrusive data and to record how such an assessment had been reached.

33. All bulk personal dataset authorisation forms are held on the corporate record and are subject to review by the Intelligence Services Commissioner. All BPD must be authorised using the authorisation procedure. SIS does not seek to acquire BPD unless it has the intention to exploit it.

RETENTION PERIODS

34. In October 2007, it was agreed internally that datasets should be subject to regular reviews. The first Dataset Retention Review was held in June 2008 (two datasets were subject to individual reviews in the interim).

35. The Panel meets every six months (and has done since its inception, with one exception) to review BPD holdings and to ensure that a necessity and proportionality case for retaining datasets can be made. Where it cannot, the Panel directs that datasets are deleted. The Panel has the option to remove datasets from the main database and retain for future re-ingestion if a case can be made. This option has not been used since November 2013; the Panel instead preferring to delete data for which a case cannot be made. The Panel is chaired by a senior member of staff and includes legal and policy representation. Representatives of MI5 and GCHQ regularly attend. The Panel considers usage statistics, evidence of operational impact and weighs this against the content of the dataset and the level of intrusion that it represents.

36. Until October 2015 every bulk personal dataset was reviewed every six months. From October onwards, datasets are assigned to a review period based on their level of intrusion. Datasets assessed to represent a high level of intrusion are reviewed every six months. Medium intrusion datasets are reviewed at least every 12 months and low intrusion datasets at least every two years. A dataset may be assigned to a more regular review period than its level of intrusion would otherwise dictate because, for example, it is rated as high risk (although it cannot be assigned a less regular review period on the basis of lower risk). This change was discussed with the Intelligence Services Commissioner who noted that it was in line with practice at MI5.

SECURE SYSTEMS AND STORAGE OF DATA

37. All SIS systems are subject to Security Department access control and audit measures. Users are required to hold developed vetting status and apply for access to systems with line manager approval. All users are issued with individual password-protected logins and required to sign the relevant Security Operating Procedures (SECOPS) (see SIS exhibit pages 111-118) and all systems are audited for unusual or inappropriate activity. SECOPS for systems are developed for security rather than compliance purposes but demonstrate a level of safeguard around access control and individual responsibility for IT activity. If an individual moves to a new role, their access to the system ceases at the time of that move. If their new role requires access to the database, a new application must be submitted and the Codes of Practice and SECOPS must be re-signed.

38. As described above, the evolution of the bulk personal data capability was a gradual one. Initially focussed on CT operations, the capability began to grow in terms of numbers of datasets and users. The potential benefits of aggregating data became increasingly clear and SIS identified a need for a tool to hold, connect and analyse this data. The database, plus the surrounding policies and procedures for access and audit, were designed from the outset to be compliant with the relevant legal and policy concerns.

39. Since the introduction of the database in 2009, users have been required to submit a business case when applying for access. In August 2010, SIS introduced a Code of Practice (see SIS exhibit pages 101-104) which all users must read and sign. The tool itself contains a prompt before the user can access any material, which reiterates their responsibilities. All users are required to undertake the appropriate training on IT systems. Mandatory training on SIS's main analytical tool includes legal and policy considerations and methods for reducing collateral intrusion during searching.

40. In February 2011 a new audit process was implemented that included the issuing of audit justification requests to users on a random, untargeted basis. In April 2011, the

system was further expanded to issues audit justifications for users who had triggered particular system algorithms around inappropriate use.

41. Since October 2014, users have been required to record a specific justification for each search that is conducted on the system. Since October 2015 this has included a mandatory acknowledgement that the user has considered other, less intrusive means to achieve their objective.

SAFEGUARDS BUILT INTO THE ELECTRONIC INTERFACE

42. The database contains warning notices that any member of staff must read and accept before using the system. Between the delivery of the system in 2009 and June 2011, the login prompt read as follows:

"This system may be used for authorised purposes only. All information on it belongs to HMG and may not be accessed without prior authorisation. The Service will audit and monitor information on this system. An individual user has no legal right to absolute privacy on this system. Any misuse of this system will be handled as a disciplinary matter. By continuing to logon you consent to these conditions."

43. Between June 2011 and October 2014, the login prompt read:

"Access to the database is strictly controlled and all searches subject to scrutiny by the Intelligence Services Commissioner and Security Department. You should ensure that your use of the system is related to your work and that using the database is necessary and proportionate. Misuse of the database data could amount to criminal offence and may lead to disciplinary action.

- **Recording the database information.** When you use information in correspondence you must apply the relevant file reference in addition to the main file reference. This is a file used to capture outcomes from the database.

- **Disseminating the database information.** You may pass all database results to GCHQ and BSS without need for Action On, as long as you state the source and classification of the data. [redacted]

- **Retaining target knowledge.** [redacted]

- **Handling inaccuracies.** Bulk data can occasionally contain errors. If you identify something which looks untrue or incomplete, you should inform [redacted] ASAP so that it can be investigated/corrected.

For further information, please refer to the database Code of Practice on the intranet."

44. Action On is the process whereby a customer requests permission to make active use of SIS intelligence. When seeking to pass any data derived from the database outside of the SIA, SIS must be satisfied that it is necessary for National Security reasons to pass this data, and proportionate to do so for that purpose. It will not normally be considered necessary to pass data to an agency which could obtain the same data from another source.

45. The login prompt encourages staff to record the database information substantively in order to ensure that all actions resulting from any search of bulk data are saved to the corporate record and so that SIS is able to demonstrate necessity and proportionality considerations for legal and compliance purposes.

46. Since October 2014, the database login prompt has read as follows:

"Your access to and use of the data in the database are likely to represent an intrusion into individuals' privacy. The Human Rights Act requires your actions to be necessary for the purposes of SIS's functions and proportionate to what we are seeking to achieve. All queries require a justification that explains clearly why this search contributes to meeting a specified intelligence requirement.

Access to the database is strictly controlled and all searches subject to scrutiny by the Intelligence Services Commissioner and Security Department. You should ensure that your use of the system is related to your work and that using the database is necessary and proportionate. Misuse of the database data, including unjustified and/or inappropriate access, would be unlawful and could amount to a criminal offence. The Service will take disciplinary action where the database data is searched inappropriately by staff.

All users have signed the database Code of Practice and by clicking 'Accept' you are reconfirming your agreement to abide by it."

47. The database has been built with necessity and proportionality in mind. Since October 2014, prior to running a search, users must provide a justification for running each search:

"To comply with the Human Rights Act you must be able to justify your search is necessary for and proportionate to the purpose you have selected. What is the intelligence requirement for this search? [redadcted]

Purpose [user must select one from the following drop down list: NS - National Security, EW - Economic Wellbeing, SC - Serious Crime]

Necessity [user must complete a free text box according to the instructions]"

48. In October 2015, a tick box was added which required the user to read and agree:

"I consider this search to be proportionate and there is no less intrusive means to achieve the same objective"

The information entered into the necessity box is available to the Commissioner in the course of his scrutiny work. Searches are also subject to internal audit by the Security Department.

49. The database has been designed deliberately to promote considerations of proportionality and to limit the user where possible, without damaging the tool's operational effectiveness. The tool is expressly designed to enrich knowledge of known targets rather than search for new ones. Users are not able to conduct broad, profiling-type searches. A search can only begin with a piece of lead intelligence e.g. a selector connected with a subject of interest. Searches allow a user to find other instances of that selector and supplement their knowledge of the subject of interest. The tool ensures that the vast majority of data will never be viewed by an analyst and reduces the level of actual and collateral intrusion to a minimum.

TRAINING AND GUIDANCE

50. All staff must undergo training on the database as part of the application process before they can be granted access to the system. This mandatory training outlines the legal and ethical responsibilities of all staff in accessing bulk personal data and reinforces the messages in the Code of Practice. Advanced analysts complete not only mandatory training but also supplementary training, which includes guidance to support them in their authorisation, transformation and analysis tasks. All applications for a database account must be approved by the appropriate line manager before they can proceed.

51. The first version of the Code of Practice was introduced in August 2010 (see SIS exhibit pages 101-104). It outlined the responsibilities of all staff in accessing data through the database. In April 2011, it was updated with minor amendments (see SIS exhibit pages 105-108). In November 2011 it was updated to include a section on responsibilities of line managers and was reissued to all staff to ensure they had read and signed the latest version (see SIS exhibit pages 33-36). In October 2014, the Code was updated to reflect changes in functionality i.e. the introduction of the mandatory necessity box (see SIS exhibit pages 37-40). In November 2015, minor amendments were made for clarity and to reflect that access to the system is revoked when a user moves jobs or changes role (see SIS exhibit pages 41-44).

52. Before October 2011, all users were required to submit a written justification for their request on applying for access (see SIS exhibit pages 109-110). In October 2011, the form was amended (see SIS exhibit pages 45-46) as follows:

"The database contains sensitive personal data and access to it is controlled. Please explain why your post requires access and how it will provide operational value. Please provide 2 or 3 lines, briefly describing how you might use the database."

53. In October 2014, the application form was updated (see SIS exhibit pages 47-48) as follows:

"The database contains sensitive personal data, including on individuals who are not deemed to be of intelligence interest. Given the potential for intrusion into privacy, access to the application is controlled and only extended to users whose access to the data is necessary and proportionate to the Service's functions in law. Access to the database is specific to an individual's role and will be removed when you change post, after which you would be required to re-apply for access, if necessary, based on your new role.

Please explain how you would use the database in your current role: [text box]

Please explain why your use of the database would be necessary for the Service to exercise its functions for the purposes of national security, the economic wellbeing of the UK or the detection/prevention of serious crime: [text box]

How would your use of the database be proportionate to fulfilling the Service's functions - for example is there a less intrusive way for you to achieve the same objective without access to the database data? [text box]"

54. In October 2015, further functionality was added making it mandatory for a user to confirm consideration had been given to proportionality before conducting a search.

55. In addition to formal training, the Data Directorate and/or the Security Department have occasionally delivered compliance messages to the database users. These have taken the form of newsletters or notices sent via email to all users, messages and documents on the intranet and more formal staff notices which are circulated to all staff and placed on the corporate record (see SIS exhibit pages 55-56 and 85-90). They are supported by pages on the intranet (see SIS exhibit pages 57-64) detailing the policies and procedures surrounding access to bulk personal data and the database.

56. In March 2016, SIS instituted a bulk personal data compliance test that is mandatory for all staff who will work with BPD. Staff must pass the test before applying for a live account and all staff will be required to retake the test at least every two years.

57. Best practice messages around working with bulk personal data are included in a number of SIS's standard courses. Representatives from the Data Directorate speak on induction, intelligence delivery and targeting courses. All staff in the senior management cadre must take and pass a 'Legal Compliance with Data' course.

INDEPENDENT OVERSIGHT

58. In February 2010, the Intelligence, Security and Resilience Group at the Cabinet Office undertook a review of the Agencies' handling of bulk data. In the course of 2010 informal discussions and briefings took place and in August SIS provided the Intelligence Services Commissioner with a copy of the SIS bulk data policy, an example authorisation form and summary of the Data Retention Review process. In October 2010, the Prime Minister wrote to the Commissioner asking him to take on oversight of the Agencies' use of data on a non-statutory footing. He has incorporated this oversight at his biannual scrutiny visits since December 2010. This oversight was placed on a statutory footing under a direction issued by the Prime Minister in October 2015 (see SIS exhibit pages 135-136).

59. The Commissioner has carried out twelve scrutiny visits on BPD since October 2010 in addition to receiving other briefings and demonstrations of analytical tools. At each visit he randomly selects at least two searches of the database and meets with the officers who carried out the search to examine the justification. He is provided with a full list of advanced analyst tasking and selects up to six tasks. He meets with the tasking officer, the relevant analyst and reviews all associated paperwork. He selects approximately 15 datasets from the full list of holdings and scrutinises the related authorisation paperwork. He also selects a number of audit challenges and reviews the original search, the audit team response and the outcome. He is additionally provided with any audit challenges that have resulted in a breach. He has been provided with all applicable policies, procedures and safeguards and any significant changes to handling arrangements are brought to his attention. SIS has sought, or he has provided, his advice on a number of policy and handling issues including the format of forms for authorisation and tasking and the adequacy of procedures for retention, review and audit. SIS has updated forms and improved its processes in the light of his comments, for example providing mandatory means for recording necessity and proportionality and meeting his targets to improve the time taken to complete authorisations.

60. The Agencies gave detailed evidence to the Intelligence and Security Committee's Privacy and Security Inquiry in early 2014. Prior to that date SIS responded to queries and request for briefings on bulk data in the normal course of business.

NON-COMPLIANCE

61. All staff are aware that searches of the database are subject to audit procedures. They are aware that audit requests are issued by the Security Department and that the Commissioner picks a number of the database searches for review during his scrutiny visits. Audit requests are issued because a search has met particular criteria that act as a trigger; random requests are also issued. Each audit request is investigated. Examples of non-compliance are very rare and have serious consequences including disciplinary proceedings, the serving of security breaches (placing a formal record of a breach on an individual's personnel file, which could impact appraisals and eligibility for postings etc) and dismissal. Less than 1.5% of audits have resulted in the discovery of any non-compliance.

62. The claimants evidence has referred to a summary of communications with the database users (which was previously disclosed as historical tab 21 and is exhibited to this statement as SIS exhibit pages 85-90). The matters referred to in that document are as follows: a user searching for an address for a family member's birthday card, a search for passport details for a colleague in order to book his travel, and a search to identify a date of birth for personal reasons related to clearance. One user was discovered to have searched bulk personal data in relation to a colleague on a number of occasions; their contract was immediately terminated and SIS notified the Intelligence Services Commissioner. As a result of these instances of non-compliance a staff notice was issued reminding all staff of their obligations, an additional newsletter was sent to all database users and the Code of Practice was updated and re-issued; all users were required to read and sign (see SIS exhibit pages 85-90).

63. During the period 1 June 2014 to November 2015, five instances of non-compliance were detected. Two of these instances related to bulk personal datasets being ingested into the database before they were authorised. This was due to an ambiguity within SIS's systems, and changes have since been made to prevent this error from happening again. In both cases, the datasets were removed as soon as the error was detected. The remaining three instances related to individual non-compliance, by three members of staff. None of the three staff members were prosecuted or dismissed, but all were disciplined for non-compliance. Each of these three instances were identified by SIS's Information Security audit.

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

SIS Witness

Dated: 11 July 2016