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

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