

*Gists are italics double underlined
Amendments are highlighted

Witness: GCHO Witness
Party: 3rd Respondent
Number: 8
Exhibit: GCHO13-15
Date: 15.12.17

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

RE-AMENDED WITNESS STATEMENT OF GCHQ WITNESS

I, [Redacted], 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. This is my [Redacted] CLOSED witness statement in these proceedings. I have also prepared a number of OPEN statements.
2. I am authorised to make this witness statement on behalf of GCHQ. 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. I make this statement to respond to a number of points that have arisen recently in correspondence between the Tribunal and the Investigatory Powers Commissioner's Office, and that arose at the OPEN hearing on 15-17 October 2017. The particular issues are as follows:

- a) Clarification of points made in my seventh OPEN Witness Statement in relation to IOCCO s.94 audit.
- b) Provision of the paperwork that accompanied s.94 Directions when they were initially triggered.
- c) An update on the BPDs held by GCHQ and how we use them, including what techniques we use to analyse them.
- d) Details of GCHQ's holdings of social media data in BPDs.
- e) A description of GCHQ's use of Artificial Intelligence techniques with regards to BPD and BCD.
- f) Additional information regarding remote access to BPD and BCD.
- g) Additional information on the transfer of BPD and BCD.
- h) Correction and clarification of the situation regarding systems administrators.

**A. CLARIFICATION OF POINTS MADE IN SEVENTH OPEN WITNESS STATEMENT
IN RELATION TO IOCCO s.94 AUDIT**

4. My seventh OPEN Witness Statement dated 18th October 2017 corrected a statement made at page 7 of the IOCCO report of their audit inspection of GCHQ conducted on 25-26 April 2017 under s.94 of the Telecommunications Act 1984. Paragraph 4 of my Witness Statement sets out the three elements which are captured and used for auditing purposes, namely (i) the authorised purpose for which they are conducting their search; (ii) an internal cross-reference which equates to a specific intelligence requirement; and (iii) a justification of the necessity and proportionality to access the data. Paragraph 5 of the Statement states that these three elements are made available

to the Compliance Team, the IT Security Team and are provided to the IOCCO inspectors on demand.

5. Due to the wording of the recommendation in the IOCCO report, in the course of his submissions on 19 October 2017, the Claimant's Counsel interpreted this to mean that the IOCCO inspectors were only provided with the necessity and proportionality statement (element (iii) above) if they demanded to see it. This was not the case. The IOCCO inspectors saw all three elements as outlined above, which included the necessity and proportionality statements. What "on demand" refers to here is the fact that the audit logs are additionally made available to IOCCO (and now IPCO) inspectors on any occasion outside of audit inspections, should they ask to see them. For the avoidance of doubt, the complete set of query data (statutory purpose, intelligence requirement, free-text justification) is included by default in the information provided to the inspectors when they conduct their annual audit review of the use of s.94 data.
6. There was a recommendation from the IOCCO inspectors that search terms should be included in the audit logs that they review and this change was implemented in June 2017 as described in paragraph 6 of my seventh Witness Statement.

B. PAPERWORK ACCOMPANYING s.94 DIRECTIONS

7. My fourth OPEN Witness Statement dated 16th June 2017 describes the process by which s.94 directions have been made and communicated to the CSPs to which they relate. Paragraph 9 explains that the provision of data under s.94 directions is triggered initially by a request from the Director of GCHQ. I attach as exhibit GCHQ13 a selection of triggering letters for the assistance of the Tribunal. All of the triggering letters sent from Director to the CSPs were substantially identical to these.
8. It will be noted that there was a period of 7 weeks between the signing of Directions on 29 November 2001 and the sending of letters to the CSPs on 17th January 2002. The reason for the delay has not been documented but appears to be purely bureaucratic: records of internal emails show that 4 working days after the Direction was signed work was underway to draft and send the letters to the CSPs and it was acknowledged that this needed to be done swiftly. The note relating to the October 2016 Direction is

undated but the metadata on GCHQ's EDRM system indicates that it was created no later than 17 October.

C. UPDATE ON THE BPDs HELD BY GCHO AND HOW WE USE THEM, INCLUDING WHAT TECHNIQUES WE USE TO ANALYSE THEM

[Redacted]

9. Paragraphs 9-11 of my third OPEN Witness Statement dated 2nd March 2017 explains how we use BPDs and paragraphs 33-44 give some specific examples.
10. During the OPEN hearing the Claimant's Counsel suggested that BPDs are used for the "profiling of entire populations and looking into behaviours." Whilst BPD is held about a large number of individuals, analysts will only actually look at the data relating to a small minority of those individuals. This is because of the way in which the BPD tools work: analysts ask specific questions of the data to retrieve information of intelligence value. For example, analysts might use travel-related BPDs to track the movement of targets, detect exploitable travel patterns of targets, identify new (previously unknown) targets, or infer activities/events of interest. [Redacted]. The purpose of this activity is to allow the analyst to establish the travel activities of a specific individual. It does not result in the creation of "profiles" of individuals not of intelligence interest.

D. GCHO'S HOLDINGS OF SOCIAL MEDIA DATA IN BPDs

11. During the OPEN hearing, the Claimant's Counsel suggested that "social media" consisted of:

"not just Facebook; it is dating websites, apps and many other very sensitive sources. Such datasets, particularly if they're held in bulk, are highly intrusive, and they do contain information right at the very core of an individual's private life."

12. I am unable to confirm or deny whether or not GCHO holds social media BPDs.
13. The ways in which a GCHQ analyst might use a social media BPD is to identify individuals who are of interest for a specific reason such as those using particular keywords, travelling to particular places, interacting with particular individuals or to

gain behavioural insight into targets. Every query must be accompanied by a necessity and proportionality statement.

14. GCHO might also use a social media dataset to conduct research into improving analytical techniques and processes.

[Redacted]

E. USE OF ARTIFICIAL INTELLIGENCE WITH REGARDS TO BPD AND BCD

15. In the course of the OPEN hearing the Claimant suggested that the SIA make use of "artificial intelligence techniques" which, based on IPCO's response by email of 10 October to the Tribunal's letter of 2 October 2017, are not audited by the commissioners.
16. Paragraph 8 of the Security Service's [Redacted] Witness Statement dated 14 November 2017 gives a definition of the term artificial intelligence (AI) as it is used and understood by the SIA.
17. I am unable to confirm or deny whether GCHO carries out machine learning techniques when conducting BPD/BCD searches. Two things should be noted regarding machine learning solutions (i) they can be very accurate, but only in proportion to the volume of truthed prior data, and this is typically expensive to generate (it often requires human input to have made judgments on the example data); (ii) because they entail approximation, they can yield false positives. For this reason, they are often used for volume reduction [Redacted] rather than as the basis for decision making.

F. REMOTE ACCESS TO BPD AND BCD BY INTERNATIONAL PARTNERS.

[Redacted]

G. ADDITIONAL INFORMATION ON THE TRANSFER OF BPD AND BCD

18. To the fullest extent possible, the safeguards that GCHO would apply were it to share BPD and BCD would be the same as those it applies when sharing intercepted material. These arrangements were the subject of Sir Stanley Burnton's review of the sharing of intercepted material and related communications data with international partners. This review also explicitly addressed the possible sharing of BCD. I exhibit as GCHO15 the letter that I sent to Sir Stanley on 10 June 2016 describing the documentation that GCHQ provided to him for the purposes of this review and GCHQ's internal file note of the inspection visit from 14 November 2016. That file note recorded Sir Stanley's view that all our 5-

EYES arrangements were properly documented, and that he especially liked the post-RIPA letters sent out at the last major legislative change.

H. CORRECTION AND CLARIFICATION REGARDING SYSTEMS ADMINISTRATORS

19. In my seventh OPEN Witness Statement dated 18th October 2017 I explained in paragraph 10 that for some systems contractors may have administrator rights (known within GCHQ as a "Privileged User" (PU)). I explained that contractors only have privileged access during the design, build and testing phase and that once that was complete the administrator rights were passed to members of GCHQ staff. This is no longer the case. Following a change in policy introduced a few years ago there are contractors within GCHQ who are administrators of operational systems. This is because much of the hardware and software for these systems is provided by industry partners and they are therefore best placed to support those systems.
20. Privileged User accounts are divided into two categories, Privileged User Data and Privileged User Function. The policy governing the management of Privileged Users is exhibited as Exhibit GCHQ14.
21. PU Data access for staff who have been with GCHQ for less than 12 months and PU Function access where staff have been with GCHQ for less than 6 months is by exception and needs to be approved by the data owner.
22. Currently there are about 100 contractors with PU accounts for the main BPD and BCD repositories.
23. During the course of the OPEN hearing on 17 October 2017, the Claimants' Counsel submitted that there was nothing to stop "*a contractor with system access rights going to the system, getting the relevant data, and then covering their tracks*". The likelihood of that happening is low for the following reasons.
24. Command line interfaces (an interface which relies on the user typing commands into the computer, rather than interacting with a user-friendly interface using mouse and keyboard as one would do for example with Microsoft Windows software) are used by the PU community to manage the system (e.g. installing software patches, monitoring performance, investigating problems). There is system monitoring and auditing for malicious behaviours at the command line level. Additionally, the

presentation of information using this interface is very basic. In order to do a simple search on the data you would need to consider the following:

- i. The data needs to be stored in a format which can be searched using a text string, or be converted into such a format
 - ii. Typically the data at rest on the data storage and retrieval platforms is not in a format which can be interpreted using the command line. The data is hosted in specialist file systems, databases or applications which hold the data in such a way as to optimise the data for the analysis being carried out using the appropriate managed interfaces.
 - iii. A simple example would be a Microsoft Word document which if accessed via the command line returns a garbled set of characters because the data needs to be placed through a Microsoft office converter to present the information into a readable textual format. The file would only be viewable as a proper document with the original layout and formatting if Word itself (or a compatible application) was used.
 - iv. The data needs to be stored in such a way to allow identification of a specific desired data item i.e. a data item may not be stored in one place, rather being distributed across a number of storage servers, which can only be reassembled using the specialist software.
25. The search tools available via the command line are basic and considering the scale of data which needs to be searched against they would time out (the search would fail due to exceeding the maximum time allowed by the system) or take an unreasonably long time to return any results.
26. Although the technical community would state in theory that it is at times possible to search for a string (e.g. a name) within the data using the command line, in practice this is not how the interface is used nor is the interface designed to enable this kind of use. Typically within GCHQ the level of complexity of the systems means the only way to access the data in a readable format is via the software APIs where necessity and proportionality auditing is implemented.
27. This is how system support is carried out within technical communities across the industry and it is considered reasonable behaviour. The additional training, screening and guidance we provide to those with PU access is there to enable compliance with the desired behaviours.

Statement of Truth

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

ECMR Witness

Dated: 16 December 2017



Mr K R Tobitt
The Director

[REDACTED]

Government Communications Headquarters
Priors Road Cheltenham GL52 5AJ
Telephone 01242 (Cheltenham) 221491 ext 2010
GTN 1366
Fax No: 01242 226816

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

27 March 1998

[REDACTED]

[REDACTED]

[REDACTED]

REQUEST FOR CALL ASSOCIATED DATA

Telecommunications Act 1984, Section 94(1)

1. In accordance with the direction under the above Act made by the Secretary of State for Foreign and Commonwealth Affairs on 23 March 1998, I hereby request [REDACTED] to provide data generated by or available to [REDACTED] associated with communications being or that have been conveyed by means of [REDACTED]'s Public Telecommunications Systems in the United Kingdom, where the communications to which the data relates are the following:
 - a. [REDACTED]
 - b. [REDACTED]
2. The requirement resulting from this request will lapse after six months from the date of this letter unless the request is renewed or modified, or on an earlier written notification to [REDACTED] of such a lapse.

John Rowley
Kerri Rowley

Copies to: [REDACTED]

[REDACTED]



[REDACTED]

Government Communications Headquarters

Priors Road Cheltenham GL52 5AJ
Telephone Cheltenham (01242) 221491 ext 6106
G1N Number 1366 ext 6106

[REDACTED]

GCHQ reference [REDACTED]

Date
09 August 1999

REQUEST FOR CALL ASSOCIATED DATA.

Telecommunications Act 1984, Section 94(1)

Reference a. [REDACTED] of 22 March 1999
b. [REDACTED] of 27 March 1999

1. On 22 March I wrote advising you of GCHQ's intention to seek authorisation from the Secretary of State for Foreign and Commonwealth Affairs of a modification to the existing direction under the Telecommunications Act 1984, Section 94(1).
 2. I am now able to inform you that the new and modified direction under the above Act was made by the Secretary of State on 4 August 1999; the original is enclosed. The new direction supersedes the previous direction sent to you under reference b.
 3. In accordance with the new direction I hereby request [REDACTED] to provide data generated by, or available to [REDACTED], associated with communications being or that have been conveyed by means of [REDACTED] Public Telecommunications Systems in the United Kingdom, where the communications to which the data relates are either or both of the following:
 - a. [REDACTED]
 - b. [REDACTED]
- [REDACTED]

[REDACTED]

4. The requirement resulting from this direction will lapse after six months from the date of this letter unless the request is further renewed or modified, or on earlier notification to [REDACTED] of such a lapse.

[REDACTED]

Deputy Access and Task Control

Copied to [REDACTED]
[REDACTED] to see on file [REDACTED]

[REDACTED]

[REDACTED]

Directions to [REDACTED] under section 94(1) of the Telecommunications Act 1984

After consultation with you, and in pursuance of section 94(1) of the Telecommunications Act 1984, I hereby give to you the following directions, being directions which appear to me to be requisite or expedient in the interests of national security:-

1. [REDACTED] shall, if requested to do so by the Government Communications Headquarters (GCHQ), acting through the Director of GCHQ or any person authorised by him to make, renew or modify such requests and previously notified to [REDACTED] as being so authorised, provide to GCHQ as requested data generated by or available to [REDACTED] associated with communications being or that have been conveyed by means of [REDACTED] Public Telecommunications Systems in the United Kingdom where the communications to which the data relates are either or both of:

(a) [REDACTED]

(b) [REDACTED]

2. I am of the opinion that disclosure of these directions is against the interests of national security.

Robin Cook

One of Her Majesty's Principal Secretaries of State

Date: 9.8.99

[REDACTED]



[REDACTED]

GCHQ

Priors Road Cheltenham GL52 5AJ
Tel: 01242 221491 ext 2010
Brent: 01242 540501
Fax: 01242 256330
GTN: 1366 ext 2010
E-mail: [REDACTED]

Francis Richards
The Director

[REDACTED]

17 January 2002

[REDACTED]
Company Secretary
[REDACTED]

[REDACTED]

REQUEST FOR CALL ASSOCIATED DATA

Telecommunications Act 1984, Section 94(1)

1. In accordance with the direction made under the above Act by the Secretary of State for Foreign and Commonwealth Affairs on 29 November 2001, I hereby request [REDACTED] to provide data generated by, or available to [REDACTED], associated with communications being or that have been conveyed by means of [REDACTED]'s public telecommunications system in the United Kingdom. The data provided will relate to -

(a) [REDACTED]

(b) such other communications (if any) as necessary in order to provide the data relating to (a) above.

2. The requirement resulting from this direction will lapse after six months from the date of this letter unless the request is further renewed, or on earlier notification to [REDACTED] of such a lapse.

Yours sincerely,
[Signature] [REDACTED]

[REDACTED]

Directions to [REDACTED] under section 94(1) of the Telecommunications Act 1984

After consultation with you, and in pursuance of section 94(1) of the Telecommunications Act 1984, I hereby give to you the following directions, being directions which appear to me to be requisite or expedient to protect the United Kingdom from terrorist threat in the interests of national security: -

1. [REDACTED] shall, if requested to do so by the Government Communications Headquarters (GCHQ), acting through the Director of GCHQ or any person authorised by him to make such requests and previously notified to [REDACTED] as being so authorised, provide to GCHQ as requested data generated by or available to [REDACTED] and associated with communications being or that have been conveyed by means of a Public Telecommunication System (PTS) and data concerning the topology and configuration of [REDACTED]'s PTS. The data provided will relate to -
 - (a) [REDACTED]; or
 - (b) [REDACTED]; or
 - (c) [REDACTED]; or
 - (d) [REDACTED]; or
 - (e) such other communications or data (if any) as necessary in order to provide the data relating to (a) to (d) above.
2. I am of the opinion that disclosure of these directions is against the interests of national security.
3. I believe that this direction is necessary in the interests of national security and that the conduct directed is proportionate to what is sought to be achieved by that conduct, in particular having regard to the arrangements currently in place for meeting the requirements of section 4(2)(1) of the Intelligence Services Act 1994.

One of Her Majesty's Principal Secretaries of State

Date: *Johnathan*
29 Nov 2001

[REDACTED]



Francis Richards
The Director

[REDACTED]

GCHQ

Priors Road Cheltenham GL52 5AJ

Tel: 01242 221491 ext 2010

Brent: 01242 340501

Fax: 01242 256330

GTN: 1366 ext 2010

E-mail: [REDACTED]

[REDACTED]

17 January 2002

[REDACTED]
Company Secretary

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

PROVISION OF CALL ASSOCIATED DATA

Telecommunications Act 1984, Section 94(1)

Reference: [REDACTED] of 3 October 2001

1. The purpose of this letter is to give you notification of the arrangements that will apply to the provision to GCHQ of call associated data in the interests of national security.

Background

2. On 3 October 2001 GCHQ wrote to [REDACTED] (reference) thanking the company for the help and support it had provided following the terrorist attacks on 11 September. We pointed out that the data you had supplied to GCHQ had been provided legally under the terms of section 45(2) of the Telecommunications Act 1984 and under sections 28 of the Data Protection Act 1998. However, we believed that for future requests, you would be provided with more reassurance if you were served with a direction under section 94(1) of the Telecommunications Act.

[REDACTED]

[REDACTED]

[REDACTED]

First Formal Request for Data

3. Following consultation, a direction under the above act was made by the Secretary of State for Foreign and Commonwealth Affairs on 29 November 2001 and delivered to [REDACTED] (photocopy attached). Accordingly, I enclose a letter requesting the first supply of data under the terms of this direction. This initial request relates to the provision of a regular supply of [REDACTED] data [REDACTED] using [REDACTED]'s network. As agreed for any regular feed of data, this request will lapse after 6 months unless renewed by the Director of GCHQ or one of his nominated senior managers. This first request is for data that will have the GCHQ code word [REDACTED]

Subsequent Requests & Revalidation of Requests

4 Revalidation of the request for "CODEWORD" data, any other future requests for data under this direction, or revalidation of future requests will ordinarily be signed on my behalf by one of the following senior staff, and will be addressed to

[REDACTED]

[REDACTED]

Head of Access and Task Control
Deputy Access and Task Control
Deputy Access and Task Control

I will advise you of any changes to this list in the future. Please also be assured we will always consult your company first before making any further new requests for data

5 I am grateful to you and your staff for your continuing support. I know that the data provided under "CODEWORD" will prove a valuable aid to countering terrorist operations in the UK and safeguarding national security. Thank you for contributing to this important work.

Bill Murray
Simon L. [unclear]

[REDACTED]



Francis Richards
The Director

GCHQ

Priors Road Cheltenham GL52 5AJ

Tel: 01242 221491 ext 2010

Brent: 01242 540501

Fax: 01242 256330

GTN: 1366 ext 2010

E-mail: [REDACTED]

[REDACTED]
17 January 2002

[REDACTED]
Company Secretary & Legal Director
[REDACTED]

REQUEST FOR CALL ASSOCIATED DATA

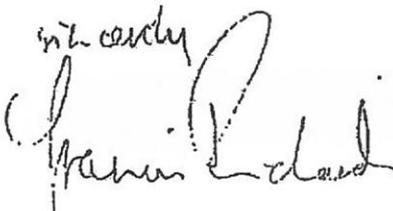
Telecommunications Act 1984, Section 94(1)

1. In accordance with the direction made under the above Act by the Secretary of State for Foreign and Commonwealth Affairs on 29 November 2001, I hereby request [REDACTED] to provide data generated by, or available to [REDACTED] associated with communications being or that have been conveyed by means of [REDACTED]'s public telecommunications system in the United Kingdom. The data provided will relate to -

(a) [REDACTED]

(b) such other communications (if any) as necessary in order to provide : : data relating to (a) above.

2. The requirement resulting from this direction will lapse after six months from the date of this letter unless the request is further renewed, or on earlier notification to [REDACTED] of such a lapse.

Yours sincerely




[REDACTED]

Directions to [REDACTED] under section 94(1) of the Telecommunications Act 1984

After consultation with you, and in pursuance of section 94(1) of the Telecommunications Act 1984, I hereby give to you the following directions, being directions which appear to me to be requisite or expedient to protect the United Kingdom from terrorist threat in the interests of national security: -

1. [REDACTED] shall, if requested to do so by the Government Communications Headquarters (GCHQ), acting through the Director of GCHQ or any person authorised by him to make such requests and previously notified to [REDACTED] as being so authorised, provide to GCHQ as requested data generated by or available to [REDACTED] and associated with communications being or that have been conveyed by means of a Public Telecommunication System (PTS) and data concerning the topology and configuration of [REDACTED]'s PTS. The data provided will relate to -
 - (a) [REDACTED]; or
 - (b) [REDACTED]; or
 - (c) [REDACTED]; or
 - (d) [REDACTED]; or
 - (e) such other communications or data (if any) as necessary in order to provide the data relating to (a) to (d) above.
2. I am of the opinion that disclosure of these directions is against the interests of national security.
3. I believe that this direction is necessary in the interests of national security and that the conduct directed is proportionate to what is sought to be achieved by that conduct, in particular having regard to the arrangements currently in place for meeting the requirements of section 4(2)(1) of the Intelligence Services Act 1994.

One of Her Majesty's Principal Secretaries of State

Date: *Tracy [Signature]*
29 APR 2001.

[REDACTED]

[REDACTED]



Francis Richards
The Director

GCHQ

Priors Road Cheltenham GL52 5AJ
Tel: 01242 221491 ext 2010
Brent: 01242 540501
Fax: 01242 256330
GTN: 1366 ext 2010
E-mail: [REDACTED]

[REDACTED]

17 January:

[REDACTED]
Company Secretary & Legal Director
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

PROVISION OF CALL ASSOCIATED DATA

Telecommunications Act 1984, Section 94(1)

Reference: [REDACTED], of 3 October 2001

1. The purpose of this letter is to give you notification of the arrangements that will apply to the provision to GCHQ of call associated data in the interests of national security.

Background

2. On 3 October 2001 GCHQ wrote to [REDACTED] (reference) thanking the company for the help and support it had provided following the terrorist attacks on 11 September. We pointed out that the data you had supplied to GCHQ had been provided legally under the terms of section 45(2) of the Telecommunications Act 1984 and under sections 28 of the Data Protection Act 1998. However, we believed that for future requests, you would be provided with more reassurance if you were served with a direction under section 94(1) of the Telecommunications Act.

[REDACTED]

[REDACTED]

[REDACTED]

First Formal Request for Data

3. Following consultation, a direction under the above act was made by the Secretary of State for Foreign and Commonwealth Affairs on 29 November 2001 and delivered to [REDACTED] (photocopy attached). Accordingly, I enclose a letter requesting the first supply of data under the terms of this direction. This initial request relates to the provision of a regular supply of [REDACTED] data [REDACTED] using [REDACTED]'s network. As agreed for any regular feed of data, this request will lapse after 6 months unless renewed by the Director of GCHQ or one of his nominated senior managers. This first request is for data that will have the GCHQ code word [REDACTED]

Subsequent Requests & Revalidation of Requests

4. Revalidation of the request for "CODEWORD" data, any other future requests for data under this direction, or revalidation of future requests, will ordinarily be signed on my behalf by one of the following senior staff; and will be addressed to

[REDACTED]

[REDACTED]

Head of Access and Task Control
Deputy Access and Task Control
Deputy Access and Task Control

I will advise you of any changes to this list in the future. Please also be assured we will always consult your company first before making any further new requests for data.

5. I am grateful to you and your staff for your continuing support. I know that the data provided under "CODEWORD" will prove a valuable aid to countering terrorist operations in the UK and safeguarding national security. Thank you for contributing to this important work.

Yours sincerely
[Signature]

[REDACTED]

[REDACTED]

[REDACTED]

Section 94 direction for provision to GCHQ of communications data

Further to our recent discussions I write to enclose, by way of service upon [REDACTED], the attached direction dated 14 October 2016 (the "Direction") given by the Foreign Secretary, further to section 94 of the Telecommunications Act 1984.

The Direction replaces the direction to you of 29 November 2001, which - on behalf of the Foreign Secretary - I am able to confirm is hereby cancelled. We are requesting the same data as previously, however, you will note that the Direction describes it in more detail. This is in light of recommendations made in the recent IOCCO report on section 94.

Yours,
[REDACTED]

Enclosure. Direction under section 94 of the Telecommunications Act 1984

Privileged Users Policy

I. Introduction

1 "Privileged Users" (PUs) for the purposes of this policy are those individuals who have IT system privileges that enable them to by-pass some or all of the controls that govern the access and activity of normal users. The extent of additional privilege ranges from those who have very limited additional privilege to execute specific tasks, those with additional privileges within an application, through to those with full control or "system admin" or "root" accounts.

2 Existing PUs who have gone through the previous process will be deemed to have the level of privilege required by their current post. If they change post, responsibilities or duties, then a further PU application following this process must be submitted. This policy applies to new systems; it is also to be applied to legacy systems unless an exemption is agreed with the security accreditor.

3 There are two categories of Privileged User: PU Function and PU Data. This categorisation may only be used where infrastructure, supporting operating systems and processes provide comprehensive security controls. Where comprehensive controls are not present, the required PU level is PU Data (defined in Section III below). The security accreditor can provide advice if in doubt.

4 For the purposes of this policy, sensitive information can include, but not be limited to, ECI, HR, Finance, Legal or Commercial. Information Asset Owners (link to [http://\[REDACTED\]](http://[REDACTED]))

are responsible for determining what information is sensitive.

II. Principles

P 1. The PU process must focus on those privileged activities that give rise to greatest risk.

P 2. The PU process is owned by Security who are responsible for ensuring a corporate record is held of all PUs and their level of privilege. Elevated privileges must be reviewed once a month by system managers and removed as soon as the requirement for them ends. This is in line with the GIAS Information Security Policy, Chapter 2, System Manager Guidance.

P 3. All PUs must have a Developed Vetting (DV) clearance that has been granted or reviewed and accepted, by GCHQ. Suitability to

[REDACTED]

retain PU status will be reviewed as part of the regular Security Appraisal process.

P 4. The number of PUs for any system must be kept to the smallest number consistent with business responsiveness and efficiency.

P 5. The level of additional privilege made available to any user must be kept to the minimum necessary to perform the functions required.

P 6. PUs who have full control (e.g. root access or administrator account) must have two separate accounts; the account with the additional privilege should follow User Account Authority naming conventions for distinguishing privileged accounts.

P 7. PUs must only use their privileged account for privileged functions. Those functions that require only normal levels of privilege must be performed with the "normal" account.

P 8. Projects, sponsors and security managers must identify the roles or posts that need elevated privileges and determine the required level of privilege according to Section III of this policy.

P 9. In some circumstances, PUs can impact the availability of operational systems. In such cases there must be a segregation of roles such that the PU cannot impact the system recovery process as well.

P 10. PU status is not for life - it will be removed with a change of post or responsibilities. If a PU or individual with normal privileges changes role, position or responsibility to one that requires additional privileges, the level of additional privilege must be assessed (see Section III) and an application for that PU level must be submitted. It must not be assumed that approval will be granted, particularly if individual circumstances have changed.

P 11. If new or different categories of sensitive information are introduced onto a system, individuals with PU Data status (defined below in Section III) for that system must be screened for the newly introduced sensitive information, if that has not already been done. PUs and sponsors must be aware that the sensitive information review may lead to privileged access to that system being withdrawn.

P 12. On moving post PU privileges will be removed. However, there may be a delay while the removal process takes place and individuals must not use previously held PU privileges during this time. A new application must be approved if PU privileges are required for subsequent posts.

III. Categories of Privileged User

5 Privileged Users are divided into two categories, Privileged User Data and Privileged User Function.

The PU definitions are:

- a) **PU Data:** Privileged Users who routinely access sensitive data as a result of their PU role and may require ECI, HR, Finance, Legal or Commercial briefs if deemed applicable.
- b) **PU Function:** Privileged Users who do not routinely have access to sensitive data and would either have to deliberately compromise system security, or breach the trust placed in PUs to deliberately search for sensitive data.

6 Owners and managers of Secure Access Groups are also to be considered as PUs with the level PU Function. The PU process is to be followed on change of owner or manager.

7 System Managers must consider the availability risk to their system in addition to the information risk. If a PU can prevent the normal operation of the system, segregation of duties must be enforced such that the individual cannot impact the system recovery process. Any deviation from this policy must be agreed with the Information Asset Owners whose sensitive information is on the system.

IV. Requirements for Each Category

8 Before a PU takes up their duties, the processes outlined in the following table must be completed.

Process	PU Data	PU Function
Personnel Security PU Screening	Full file review (all ECIs)	Database check
PU brief and FC300/05b signed	PU Data brief must have been completed	PU Function brief must have been completed
12 month DV review (see Para 11)	Must have been completed	Need not have been completed
Review during Security Appraisal process	Must be completed	Must be completed
Sensitive post briefing & undertakings	Must have been completed	Must have been completed
ECI, HR or finance briefings	If required by data owner	If required by data owner
COI Access	If necessary for role	If necessary for role

9 Where an individual holds a DV clearance from another vetting organisation, it must be reviewed and accepted by GCHQ before PU status may be granted. As part of that process, and in light of the individual's history, personnel security may waive all or part of the requirement for time to elapse before the DV review. Where this requirement is waived completely, the initial review and acceptance by GCHQ of the existing DV clearance effectively comprises the "12 month DV review" in the table above.

10 It is GCHQ policy to carry out a review of an individual's DV after they have spent twelve months in the Department. As an exception, Personnel Security is prepared to consider bringing the review forward to six months for PU Data, if a strong business case is presented.

11 An individual may not be granted PU Data or PU Function nor have any unsupervised access to functions requiring elevated IT privileges until the relevant process in the table above has been completed. Provided that a level of audit and accounting acceptable to the accretor is in place, they may have closely supervised access for training purposes.

12 One of the keys to managing the information risk posed by PUs is to limit the number to the minimum required while allowing the business to operate responsively and efficiently. In order to reduce the risk to system availability where a PU has the ability to negatively impact an operational system, they must not be able to impact the recovery process. Good

[REDACTED]

life-cycle management of PUs is essential risk mitigation. The process must ensure PU status is recorded and when PUs move post, or leave the department, their elevated IT privileged accesses are removed and their record updated accordingly. Fitness to retain PU status will be included as part of the annual SAF review. A great deal of trust is placed in PUs to carry out their role in accordance with GCHQ policies and this is backed up by verification from the Accounting and Audit service.

V. Compliance

13 Chapter 2 of the GIAS Information Security Policy sets out Departmental and legal liabilities:

- a) All system users are subject to this policy when using Departmental IT resources and their actions may be monitored and recorded to ensure compliance. Any identified improper or unauthorised use must be reported to line management. Significant security incidents or persistent disregard of security rules on IT facilities however discovered will be investigated by Operational IT InfoSec / Security staff. In serious cases, disciplinary action will be taken and an offender's security clearance may be restricted or withdrawn.
- b) Abuse of access rights on IT systems or networks (e.g. taking unauthorised copies of documents or modifying data without authorisation) is a criminal offence under the Computer Misuse Act 1990. The unlawful disclosure of any security or intelligence information by a Civil or Crown Servant, or by a contractor working for the Department, is an offence under Section 1 of the Official Secrets Act 1989. The Department must comply with data protection legislation according to the principles of the Data Protection Act (1998) unless exemption is necessary for reasons of national security as provided under section 28 of the Act. IT system operation should also be compliant with the Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

14 GCHQ's Behaviour and Conduct policy (link to [http://\[REDACTED\]](http://[REDACTED]))

[REDACTED]

sets out the standards of behaviour expected of anyone working for or at GCHQ and the policies that must be followed, including GCHQ's rules on security. Failure to comply with this security policy may result in the incident being reported to the Security Incident Management Team for appropriate investigative and disciplinary action being initiated by your management chain. In cases of gross or repeated misconduct, this could result in dismissal. The parent organisation of contractors and intregrees will be notified and will be responsible for invoking any formal disciplinary action.

Privileged Users Policy

I. Introduction

1 "Privileged Users" (PUs) for the purposes of this policy are those individuals who have IT system privileges that enable them to by-pass some or all of the controls that govern the access and activity of normal users. The extent of additional privilege ranges from those who have very limited additional privilege to execute specific tasks, those with additional privileges within an application, through to those with full control or "system admin" or "root" accounts.

2 Existing PUs who have gone through the previous process will be deemed to have the level of privilege required by their current post. If they change post, responsibilities or duties, then a further PU application following this process must be submitted. This policy applies to new systems; it is also to be applied to legacy systems unless an exemption is agreed with the security accreditor.

3 There are two categories of Privileged User: PU Function and PU Data. This categorisation may only be used where infrastructure, supporting operating systems and processes provide comprehensive security controls. Where comprehensive controls are not present, the required PU level is PU Data (defined in Section III below). The security accreditor can provide advice if in doubt.

4 For the purposes of this policy, sensitive information can include, but not be limited to, ECI, HR, Finance, Legal or Commercial. Information Asset Owners (link to [http://\[REDACTED\]](http://[REDACTED]))

are responsible for determining what information is sensitive.

II. Principles

P 1. The PU process must focus on those privileged activities that give rise to greatest risk.

P 2. The PU process is owned by Security who are responsible for ensuring a corporate record is held of all PUs and their level of privilege. Elevated privileges must be reviewed once a month by system managers and removed as soon as the requirement for them ends. This is in line with the GIAS Information Security Policy, Chapter 2. System Manager Guidance.

P 3. All PUs must have a Developed Vetting (DV) clearance that has been granted or reviewed and accepted, by GCHQ. Suitability to

[REDACTED]

retain PU status will be reviewed as part of the regular Security Appraisal process.

P 4. The number of PUs for any system must be kept to the smallest number consistent with business responsiveness and efficiency.

P 5. The level of additional privilege made available to any user must be kept to the minimum necessary to perform the functions required.

P 6. PUs who have full control (e.g. root access or administrator account) must have two separate accounts; the account with the additional privilege should follow User Account Authority naming conventions for distinguishing privileged accounts.

P 7. PUs must only use their privileged account for privileged functions. Those functions that require only normal levels of privilege must be performed with the "normal" account.

P 8. Projects, sponsors and security managers must identify the roles or posts that need elevated privileges and determine the required level of privilege according to Section III of this policy.

P 9. In some circumstances, PUs can impact the availability of operational systems. In such cases there must be a segregation of roles such that the PU cannot impact the system recovery process as well.

P 10. PU status is not for life - it will be removed with a change of post or responsibilities. If a PU or individual with normal privileges changes role, position or responsibility to one that requires additional privileges, the level of additional privilege must be assessed (see Section III) and an application for that PU level must be submitted. It must not be assumed that approval will be granted, particularly if individual circumstances have changed.

P 11. If new or different categories of sensitive information are introduced onto a system, individuals with PU Data status (defined below in Section III) for that system must be screened for the newly introduced sensitive information, if that has not already been done. PUs and sponsors must be aware that the sensitive information review may lead to privileged access to that system being withdrawn.

P 12. On moving post PU privileges will be removed. However, there may be a delay while the removal process takes place and individuals must not use previously held PU privileges during this time. A new application must be approved if PU privileges are required for subsequent posts.

III. Categories of Privileged User

5 Privileged Users are divided into two categories, Privileged User Data and Privileged User Function.

The PU definitions are:

- a) **PU Data:** Privileged Users who routinely access sensitive data as a result of their PU role and may require ECI, HR, Finance, Legal or Commercial briefs if deemed applicable.
- b) **PU Function:** Privileged Users who do not routinely have access to sensitive data and would either have to deliberately compromise system security, or breach the trust placed in PUs to deliberately search for sensitive data.

6 Owners and managers of Secure Access Groups are also to be considered as PUs with the level PU Function. The PU process is to be followed on change of owner or manager.

7 System Managers must consider the availability risk to their system in addition to the information risk. If a PU can prevent the normal operation of the system, segregation of duties must be enforced such that the individual cannot impact the system recovery process. Any deviation from this policy must be agreed with the Information Asset Owners whose sensitive information is on the system.

IV. Requirements for Each Category

8 Before a PU takes up their duties, the processes outlined in the following table must be completed.

Process	PU Data	PU Function
Personnel Security PU Screening	Full file review (all ECIs)	Database check
PU brief and FC300/05b signed	PU Data brief must have been completed	PU Function brief must have been completed
12 month DV review (see Para 11)	Must have been completed	Need not have been completed
Review during Security Appraisal process	Must be completed	Must be completed
Sensitive post briefing & undertakings	Must have been completed	Must have been completed
ECI, HR or finance briefings	If required by data owner	If required by data owner
COI Access	If necessary for role	If necessary for role

9 Where an individual holds a DV clearance from another vetting organisation, it must be reviewed and accepted by GCHQ before PU status may be granted. As part of that process, and in light of the individual's history, personnel security may waive all or part of the requirement for time to elapse before the DV review. Where this requirement is waived completely, the initial review and acceptance by GCHQ of the existing DV clearance effectively comprises the "12 month DV review" in the table above.

10 It is GCHQ policy to carry out a review of an individual's DV after they have spent twelve months in the Department. As an exception, Personnel Security is prepared to consider bringing the review forward to six months for PU Data, if a strong business case is presented.

11 An individual may not be granted PU Data or PU Function nor have any unsupervised access to functions requiring elevated IT privileges until the relevant process in the table above has been completed. Provided that a level of audit and accounting acceptable to the accreditor is in place, they may have closely supervised access for training purposes.

12 One of the keys to managing the information risk posed by PUs is to limit the number to the minimum required while allowing the business to operate responsively and efficiently. In order to reduce the risk to system availability where a PU has the ability to negatively impact an operational system, they must not be able to impact the recovery process. Good

[REDACTED]

life-cycle management of PUs is essential risk mitigation. The process must ensure PU status is recorded and when PUs move post, or leave the department, their elevated IT privileged accesses are removed and their record updated accordingly. Fitness to retain PU status will be included as part of the annual SAF review. A great deal of trust is placed in PUs to carry out their role in accordance with GCHQ policies and this is backed up by verification from the Accounting and Audit service.

V. Compliance

13 Chapter 2 of the GIAS Information Security Policy sets out Departmental and legal liabilities:

- a) All system users are subject to this policy when using Departmental IT resources and their actions may be monitored and recorded to ensure compliance. Any identified improper or unauthorised use must be reported to line management. Significant security incidents or persistent disregard of security rules on IT facilities however discovered will be investigated by Operational IT InfoSec / Security staff. In serious cases, disciplinary action will be taken and an offender's security clearance may be restricted or withdrawn.
- b) Abuse of access rights on IT systems or networks (e.g. taking unauthorised copies of documents or modifying data without authorisation) is a criminal offence under the Computer Misuse Act 1990. The unlawful disclosure of any security or intelligence information by a Civil or Crown Servant, or by a contractor working for the Department, is an offence under Section 1 of the Official Secrets Act 1989. The Department must comply with data protection legislation according to the principles of the Data Protection Act (1998) unless exemption is necessary for reasons of national security as provided under section 28 of the Act. IT system operation should also be compliant with the Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

14 GCHQ's Behaviour and Conduct policy (link to [http://\[REDACTED\]](http://[REDACTED]))

sets out the standards of behaviour expected of anyone working for or at GCHQ and the policies that must be followed, including GCHQ's rules on security. Failure to comply with this security policy may result in the incident being reported to the Security Incident Management Team for appropriate investigative and disciplinary action being initiated by your management chain. In cases of gross or repeated misconduct, this could result in dismissal. The parent organisation of contractors and intregrees will be notified and will be responsible for invoking any formal disciplinary action.

[REDACTED]



Hubble Road
Cheltenham GL51 0EX

[REDACTED]
Deputy Director Mission Policy

Tel: 01242 221491 Ext: [REDACTED]
Brent: [REDACTED]

GCHQ Ref: [REDACTED]

Sir Stanley Burnton
Interception of Communications Commissioner
Fifth Floor
Peel Building
2 Marsham Street
London
SW1P 4DF

10 June 2016

Dear Sir Stanley,

GCHQ RESPONSE TO RECOMMENDATION 3 FROM THE IOCCO AUTUMN 2015 INSPECTION OF GCHQ – SHARING OF INTERCEPTED MATERIAL AND RELATED COMMUNICATIONS DATA WITH FOREIGN PARTNERS

Recommendation 3 of the report on the IOCCO inspection visit carried out in November 2015 asked GCHQ to facilitate a review by IOCCO of the arrangements in place for the sharing of intercepted material and related communications data (RCD) with foreign partners. As a first step we were asked to provide you with a schedule containing the following information by 31st May 2016 (subsequently extended by agreement to 10 June):

1. Name of the partner and country.
2. Description of the type and nature of intercepted material/RCD (including where relevant the name of the system/dataset) shared.
3. Whether there is a signed memorandum of understanding or other agreement in place (if yes, please provide a copy and the date on which it was signed by both parties)
4. Whether the material/RCD shared is raw product, analysed product or end product reports (that identify themselves as intercepted material or RCD).

1 of 4

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.osi.gov.uk

[REDACTED]

[REDACTED]

5. Whether the material/RCD was shared as a historic one-off disclosure or is subject to ongoing disclosure.
 6. Where the material/RCD that has been shared is stored (i.e. at a GCHQ site or by the foreign partner)
 7. If the material/RCD is stored by the foreign partner what is the agreed retention period?
 8. Who is responsible for the deletion of the material/RCD? How is that verified?
 9. How the material/RCD is accessed or selected for examination by the foreign partner.
 10. How many queries/searches of the material and RCD are made per year by the foreign partner?
 11. What audits are in place of the foreign partner's use of the material/RCD? Provide details of the dates and results of any audits.
 12. How does GCHQ ensure that the foreign partner is not sharing GCHQ material/RCD with other agencies or conducting queries on behalf of other agencies?
2. As requested, we have set out our responses [REDACTED].
3. In addition to the list of requirements set out in paragraph 1, there were also some supplementary questions relating to communications data:
1. Is any communications data obtained pursuant to any s.94 direction shared with any foreign partner?
 2. Is any communications data acquired under Chapter 2 of Part 1 of RIPA shared with any foreign partner?
3. In respect of the first of these questions, as will have become clear from the recent s.94 review conducted by your inspectors [REDACTED].
4. I hope that the information in this letter and the attached annexes meets the requirement as set out in the inspection report. We will, of course, be very happy to discuss these arrangements with you in more detail should you feel it to be necessary.

Yours sincerely

2 of 4

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

[REDACTED]

[REDACTED]

[REDACTED]
Deputy Director Mission Policy

3 of 4

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

[REDACTED]

[REDACTED]

[REDACTED]

4 of 4

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

[REDACTED]

[REDACTED]

**Filenote of Interception of Communications Commissioner's
International Datasharing inspection of GCHQ – 14 November 2016**

[REDACTED]

1. **Review of recommendations, wrap up and conclusions.** To close the day we discussed future potential visits for Sir Stanley, who is particularly keen to visit Bude, then MHS and Scarborough, ideally accompanied by the new IPC once appointed. Sir Stanley thanked GCHQ and said that he was very appreciative, and appreciated the value of what GCHQ does. He noted that all our 5 Eyes arrangements were properly documented, and especially liked the post –RIPA letters sent out at this last major legislative change. We plan to do the same but in more detail post-IPA implementation with the aim of pre-empting any potential litigation and in a format suitable for disclosure if necessary. We can show full visibility and control of tasking on our own systems though less so when data leaves GCHQ. [REDACTED] mentioned that there had so far been no litigation on international Datasharing except for PRISM. The Compliance Guide will be rewritten, again in a format suitable for disclosure if required.

[REDACTED]

[REDACTED]