[redacted]

## Government Communications Headquarters

Datasets held at the start year: [redacted]
Datasets acquired in year: [redacted]
Datasets deleted in year: [redacted]
Datasets held at the end of year: [redacted]

GCHQ supply me with a complete list of the bulk personal data sets they hold. For those datasets I select for inspection they also supply me with copies of the minutes recording the justification for acquisition and the associated retention reviews which they carry out on a regular basis. I am satisfied GCHQ can justify retention of the data sets held by them.

GCHQ authorises the acquisition of each dataset before it is loaded into operational systems and retention of each dataset is reviewed by a panel of senior staff (including a lawyer) at least once a year (more frequently for more sensitive datasets). The business case for extended retention and the decision of the review panel are recorded in the paperwork relating to the specific dataset and this paperwork is presented to me for inspection. The majority of bulk data has historically been held on [redacted]

The case for renewal or cancellation includes:

- an assessment of the necessity and proportionality for retention
- how the data has been used
- an assessment of the benefits of the data and if these could have been achieved through other means
- the intelligence outcomes during this review period

The documentation was made available to me as were the minutes of GCHQ senior managers' regular reviews of BPD.

[redacted]



11

[redacted]

# 9. MISUSE OF DATA AND PROTECTIVE MONITORING

My oversight is limited to bulk personal data but I believe it would be helpful if I had oversight of all data obtained under the warrants/authorisations subject to my remit, including potential misuse of such data. Agencies do monitor the use of all data whether open source, targeted or bulk data holding and review the collection, retention and deletion of this data. Looking at misuse they have a mass of private information, a lot of it unused, so stringent rules need to be in place to check for and prevent misuse with strong disciplinary procedures for misuse. The chance that targeted data (from people of intelligence interest) would be misused is less but it is still personal data and it should not be accessed unless necessity can be demonstrated – there is no entitlement to misuse this data.

## Security Service

The use of bulk data within the Security Service is protectively monitored to both deter and identify inappropriate behaviour. In the event of inappropriate behaviour being identified, there are a range of disciplinary actions varying in severity that can be implemented. Furthermore, the Bulk Personal Data Review Panel (BPDRP) regularly reviews thematic issues arising from the use of bulk personal data; including consideration of usage where the necessity and proportionality might be judged marginal.

MI5's protective monitoring team explained that the message regarding misuse of data is getting through and the number of offences is on the decline. A note has been circulated to all users informing them of my recommendation endorsing MI5's policy to tighten up its procedures so that data on staff remains properly protected. The note introduced an automatic security breach if the procedures were not followed. There has not been a single breach in MI5 for access to Bulk Personal Datasets since that note was circulated.



[redacted]

12

[redacted]

The MI5 [redacted] team was created in 2009 and since that time have seen a change in culture which has resulted in a significant improvement in compliance. Over these years most cases were work related and had the best of intention but were still unacceptable. I have encouraged them to quote me if it helps make clear to people that there is no leeway. In 2014 there were no recorded instances of misuse of bulk personal data.

Protective [redacted] of other MI5 systems uncovered a number of other instances of misuse.

| | Detail | Assessment |
|---|---|---|
| 1 | 5 cases of staff forgetting to put parameters on their search [redacted] | All were issued with breach notices. [redacted] |
| 2 | 1 officer searched for information which was outside of their area out of curiosity | This was determined to be misconduct and will be on the officer's permanent record. |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

MI5 ran through the outcome of these investigations in order to provide context and reassurance around the system of protective monitoring in place. While I have oversight of data relating to my statutory remit (Bulk Data, CHIS, DSA, and Property Warrants) I explained that seeing wider areas of protective monitoring helps me to have confidence in the system as a whole.

[redacted]

[redacted]

[redacted]

The majority of the current systems containing bulk personal data are subject to protective monitoring. Furthermore, all new systems containing bulk personal data are required to have protective monitoring included in them. Whilst some legacy systems do not have an automated protective monitoring capability, spot checks are undertaken

## Secret Intelligence Service

I reviewed SIS's protective monitoring procedures. Access to [redacted] was restricted by individual user login. Giving personal login to someone else or leaving a system unattended are considered security breaches and subject to SIS's usual HR disciplinary procedures. The login is post specific so that (for example) an SIS officer working in the China team would not have access to the same information as the Russia team or staff in the security vetting team.

[redacted]

SIS also conduct manual random searches to query the justification for that search. They believe this is a strong audit which mostly focuses on breach of "need to know"

[redacted]

[redacted]

[redacted]

## DISCIPLINARY CASES

| | | |
|---|---|---|
| 1 | A query on a telephone number which was displayed on the user's desktop phone. The phone number turned out to be that of a colleague. The record was not entered. | **Serious breach** issued |
| 2 | A self search by a non-operational officer while on the [redacted] training course and the following day when they had returned to their desk. | The searches were to familiarise themselves with the system before going out to train [redacted] **Serious breach** issued. |
| 3 | A self search by a non-operational officer to retrospectively fill in a Personal Security Log with travel details following a vetting interview. Associates were also clicked on but were not entered into in any depth for system familiarisation. | Pending |

The two serious breaches were a breach of the [redacted] code of practise and classed as serious security breaches on the individual's HR record. I agreed that, although the sanction appears tough because there was no invasion into privacy, the penalty was absolutely right because both officers had undertaken an inappropriate use of the [redacted] system. SIS assured me that they had undertaken an investigation of all other searches undertaken by both users and assured themselves that these were the only incidents.

SIS confirmed that they are following my recommendation to categorise [redacted] misuse as breaches. When a query is not necessary to the role and proportionate it is a case of serious misconduct.

I was concerned that the officer searching for the contact details of a relative had retained access to [redacted] despite changing designation. [redacted] access is determined by designation which places limitations on access to data. It should

[redacted]

[redacted]

not be possible to carry this across to another designation (post). I asked SIS to explain what they are doing to ensure this has not happened elsewhere.

SIS explained that in this case IT Admin re-set the officer's password without going through the normal process which is in place to ensure that the requester is entitled to access. They do not believe that this officer was knowingly misusing the system. They hope this is an anomaly but are checking to see if it has happened elsewhere.

I tasked SIS to update me on this. I also want to see what they have done to ensure people are removed from the [redacted] register when they move post and what they are doing to ensure that IT Admin follow the correct procedure.

I was very firm in saying that unauthorised access to [redacted] must be stopped. The corporate failure in this case was a more serious breach than the misuse. [redacted] carries highly personal data and it is vital that staff only have access if they have a business need.

## Government Communications Headquarters

Use of bulk personal datasets is a relatively niche and small-scale activity for GCHQ, particularly compared to its use of material obtained via interception, but also when compared to its use of material obtained via CNE. Only a subset of GCHQ analysts have access to bulk personal datasets, and each of these staff will only have access to a subset of the datasets held by GCHQ, when those datasets are determined to be relevant to that analyst's operational targets.

All GCHQ analysts, including those with access to this data, have to complete mandatory legalities training, including a test, which reminds them of their legal obligations when examining any operational data – examination must be justified, necessary and proportionate.

For each query against a bulk personal dataset an analyst is required to briefly describe why they feel it is justified to intrude into the privacy of the



[redacted]

[redacted]

individual(s) concerned. During the November 2014 inspection I was shown the results of an audit of these 'HRA justifications', which looked at a sample of several hundred queries. While some improvements needed to be made to a proportion of the justifications, **the audit did not find any evidence that any of the queries represented an inappropriate use of the data.**

Only a handful of GCHQ's bulk personal datasets are likely to contain data relating to UK persons or persons known by GCHQ staff, thus the motivation to misuse access is likely to be minimal. There is also the deterrent presented by GCHQ's protective monitoring of access to operational systems – knowledge of the existence of this monitoring is widespread, though details of specific monitoring capabilities are tightly controlled for security reasons. Automated monitoring of the tool in which most of GCHQ's bulk personal datasets are stored has been in place since late 2011.

- **Safeguards**

GCHQ apply RIPA Part I safeguards to all data which includes protection of information of no intelligence interest, when data can be deleted and protection of confidential information.

- **Incident Management**

[redacted]

Not making a good case in the HRA justification may not mean that the action was not necessary and proportionate – it may just mean that the analyst has not set this out adequately.

There is an Information and Security Board which meets regularly to consider topics relating to Security.

Bulk Personal data is only a proportion of all operational data. Three minor breaches shown to the Commissioner did not relate to Bulk Personal Data but it was important for me to have the complete picture so as to be able to assess the effectiveness of the monitoring system.

- **HRA Audit**

Each use of GCHQ's IT system results in an invasion of privacy so the HRA justification must be completed. These justifications are audited and, if necessary investigated further by the compliance team. Saying something like "counter intelligence" is not acceptable; the analysts must set out in full why there is a requirement such as "believed to be a member of x involved in x".

I commented that this monitoring system seemed a good system. It is not an absolute guarantee but nothing could be absolute. MI5 and SIS treat any inappropriate access of personal data as a major breach and I recommended that GCHQ discuss with colleagues across the SIA to ensure consistency in approach.

[redacted]

## 10. SECTION 94

There continues to be [redacted] s94 directions [redacted] of which have been reviewed previously. One was selected for Inspection which had not previously been reviewed.

The list set out

- the name of the communications provider
- when the direction was first served
- the date of previous inspection
- a brief description of the data provided under the direction

Although there is no formal mechanism in existence to cancel a Section 94 direction once it is in place, GCHQ inform both the CSP and the Minister when they cease to rely on it.

The directions are reviewed every six months and the relevant CSP is informed of the review (this is done in writing where possible but some CSPs cannot handle classified material).

S94 product can be stored for [redacted] but most is overwritten after a few [redacted] Following a recommendation from the Interception of Communications Commissioner this is being reduced to a [redacted] storage period.

[redacted]

(d)

[redacted]

Intelligence Services Commissioner

# Report of the Intelligence Services Commissioner for 2013

CONFIDENTIAL ANNEX

The Rt Hon Sir Mark Waller

26th June 2014

Excluded from publication under section 60(5) of the Regulation of Investigatory Powers Act 2000

[redacted]



20