

[REDACTED]

time consuming to compile statistics retrospectively. To supply a three year comparison would require staff to go through a large number of security records most of which do not relate to misuse of operational data. This is not possible in time to publish my 2013 report so GCHQ have limited their statistics to incidents which have been categorised as "major".

Between 2011 and 2013 there were no major security incidents related to the misuse of bulk personal data. However, during my inspection I was given details of incidents, investigations and disciplinary steps taken as a result of misuse of other types of operational data in order to illustrate the robustness of the processes described above.

9.4 Summary of Data Misuse for the Past Three Years

MI5	Of the 191 investigations for potential misuse of data 6 were referred to HR for further investigation resulting in the issue of 4 security breaches (2 serious).
SIS	Of the [REDACTED] justification requests, 2 resulted in disciplinary referral or equivalent and 14 in the issue of security breaches (7 serious).
GCHQ	Between 2011 and 2013 there were no major security incidents related to the misuse of bulk personal data but detail of other incidents could not be obtained in the time frame available.

- One case in MI5 and one case in SIS involved a contractor and in both cases a serious breach occurred which resulted in removing the contractor from the Service.
- One case in MI5 was by a person with enhanced IT privileges who was issued with a "Minor Misconduct" charge.




Report of the
Intelligence Services Commissioner
2012

CONFIDENTIAL ANNEX


The Rt Hon Sir Mark Waller

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



©

32



Statutory and Extra-Statutory Functions


In my open report I have set out my statutory functions and one of my extra-statutory functions relating to the Consolidated Guidance to Intelligence Officer and Service Personnel on Detention and Interviewing Detainees and on Passing and Receipt of Intelligence Relating to Detainees (Consolidated Guidance). In addition to this I have been asked to oversee:

Bulk Personal Data

In 2010, my predecessor agreed to provide independent oversight of the intelligence Services' holding and use of bulk personal data which is not already overseen by the Interception of Communications Commissioner. I have developed, with the intelligence Services, a system under which I am informed of all bulk personal data sets held and of the steps taken to ensure proper and proportionate use of the same.

Section 94

Additionally to my oversight of Bulk Personal Data, GCHQ asked my predecessor to oversee the activity of GCHQ in relation to data acquired by means of directions given by the Secretary of State under section 94 of the Telecommunications Act 1984. I have continued to inspect these directions following a similar approach.



Bulk Personal Data

On 14 October 2010, the Prime Minister wrote to my predecessor, Sir Peter Gibson, requesting that Sir Peter report to him, the Home Secretary (in relation to the Security Service) and the Foreign Secretary (in relation to SIS and GCHQ) on the adequacy of policies and procedures in the agencies, and on a proposed framework for ongoing oversight by the Commissioner on an extra-statutory basis, in respect of the acquisition, retention and deletion of bulk personal data holdings and in respect of the access to and use of such data.

Sir Peter Gibson reported "In my opinion such a regime will be an effective way of providing independent oversight of the agencies' holding and use of bulk personal data which is not already overseen by the Interception of Communications Commissioner. In the case of GCHQ, the Commissioner will adopt a similar approach in respect of data acquired by means of Directions issued under Section 94 of the Telecommunications Act 1984."

Details of my Oversight of Bulk Personal Data

Security Service

At the Security Service I inspected the bulk data sets obtained, retained and decommissioned by the Security Service during my two inspections in 2012. I was also briefed on the guidance, instructions and terms of use given to all Security Service staff with access to key bulk datasets, and on associated vetting issues. I reviewed the work of the Security Service's internal systems audit team who are charged with investigating any incidents of suspected misuse. I was satisfied with these briefings and the paperwork inspected.

My particular concern was to confirm that a robust procedure was in place to establish any misuse and to monitor the same. I was satisfied that there was such a process. I received a detailed report showing how the auditing procedures were effective to catch even innocent misuse and this is now an established part of my scrutiny visits.

SIS

I was briefed on a Service-wide notice that reinforced the need for appropriate usage of SIS bulk data. This notice included a set of "Dos and Don'ts", which remains on SIS's intranet as guidance for all users. In addition, before being granted access to SIS's bulk data holdings SIS officers are required to sign Security Operating Procedures and a Code of Practice, and attend mandatory training. I was also briefed twice in 2012 on the audit systems through which bulk data searches are monitored, and this will be a standing item for all scrutiny visits.

GCHQ

I was briefed on the clear instructions given to users on the importance of not misusing in any way the powers of access to bulk personal data. I am sure that personnel are aware of this position but I am seeking clearer documentation supporting their auditing process for each of my scrutiny visits.



Recent Media Reporting

In light of recent events relating to press comment about the legality of GCHQ's activities, as I said in my open report, I discussed matters fully with senior officials within GCHQ. I will expand only a little to say that GCHQ has kept me fully informed.

I have been to visit twice (once because I was going anyway to observe a training session) and on each occasion I felt assured that there was no substance to the assertion that GCHQ was circumventing the legal framework over which I have oversight.



[REDACTED]

5b. Non-targeted bulk personal data

On 22nd October 2010, the previous Intelligence Services Commissioner Sir Peter Gibson wrote to the Prime Minister agreeing that the Intelligence Services Commissioner would take on the task of providing interim independent oversight of the intelligence agencies' holdings and use of bulk personal data in so far as it was not already the responsibility of the Interception of Communications Commissioner.

On 11th January 2011, Sir Peter submitted to the Prime Minister, the Home Secretary (with respect to the Security Service) and the Foreign Secretary (with respect to SIS and GCHQ) a report on the adequacy of policies and procedures in relation to bulk personal data holdings, and a proposed framework for the on-going oversight of this capability. As set out in the relevant section of that report, the current Commissioner has continued to pay an inspection visit to each agency every six months to review agencies' holdings of bulk personal datasets. Such visits have been an extension of his formal oversight visits in relation to the performance of his statutory duty of review.

The Commissioner can report that each of the intelligence agencies have provided to him a list of all the bulk personal datasets extant at the time of the inspection visit and details of all deletions and acquisitions of datasets in the intervening period since the last visit. The Commissioner has then been able to select from each intelligence agency a number of datasets which have been inspected during the non-statutory elements of inspection visits. The relevant agencies have also shown the Commissioner the most recent versions of their bulk data retention and acquisition policies and procedures. The Commissioner has also discussed with relevant personnel during inspections the minutes of data retention review meetings where decisions about the acquisition, retention or deletion of bulk personal datasets have been made. He has also had full access to a range of staff, from desk officers running individual queries to senior officials in charge of bulk data policy at the intelligence agencies

The Commissioner's oversight of bulk personal data holdings has deliberately been focussed on audit mechanisms established within the agencies to safeguard against the abuse of bulk data systems. To this end, the Commissioner has requested in

[REDACTED]

[REDACTED]

2011 that each of the agencies establish an internal audit scheme, reporting to him during each inspection visit of those instances where abuse has been detected or policies not complied with, focussing specifically on disciplinary or remedial measures taken against those suspected of abuse by the agency. The Commissioner can confirm that such audit mechanisms have been developed and reports on their efficacy in preventing abuse made to the Commissioner. The Commissioner has also been pleased to see the increasing capabilities and resourcing of such audit mechanisms.

The Commissioner is also content that he has been provided to his satisfaction full information on cases of abuse of systems. In relation to SIS, for example, the Commissioner discussed the case of a contractor whose employment in the Service was terminated for the misuse of bulk data-searching tools.

In conclusion, the intelligence agencies maintain, in the Commissioner's view justifiably, that without the bulk personal data now available to them they could not provide the same level of assurance. Each agency has reported the crucial role bulk personal data and the investigative mechanisms developed around it can play in identifying and tracking individual targets and target networks, including ones where the majority of members are not known and for which access to bulk personal data can be beneficial in developing or eliminating lines of enquiry. It is also clear that given each of the agencies' individual remits and working methods there are differences between their detailed policies, mechanisms and management of user behaviour in relation to bulk personal data. These remain tailored to each agency's operational methodology and working methods.

For example, differences exist in relation to the number of analysts able to access bulk personal data at each agency. At SyS, bulk personal data is searched through the same mechanism that enables intelligence exploitation, with all users having to sign up to a code of practice. In relation to SIS, for example, the ability to search against bulk data holdings is available to those analysts in operational teams who have a business need to use it. This is a minority of the service. They receive training and briefing on acceptable use of the system. Access to underlying bulk personal data itself is restricted to a handful of advanced users with additional training, including in the acceptable uses to which that access can be put. GCHQ access to bulk personal data involves filling in a HRA justification 'pop-up' screen, the contents of which are stored and audited. Other agencies place emphasis on personal and managerial responsibility which is checked through the audit mechanism.

The Commissioner is assured that the agencies continue to have sound policies, internal processes and practices to ensure that data users comply with the relevant human rights and data protection legislation. He is also assured that sufficiently robust audit mechanisms are established to minimise the risk of data being abused.

[REDACTED]

Such processes recognise the significant intrusive nature of bulk personal data holdings and in the Commissioner's view, comply with the legal requirement on each agency to ensure that it is necessary and proportionate for the agency to both acquire and retain the data, and that such data is accessed only by vetted staff with a genuine business need to do so:

[REDACTED]

FIG/FIG

18 11 11

85

From
The Rt. Hon. Sir Peter Gibson
c/o Home Office
Room 51, 5th Floor
Peel Building
2 Marsham Street
London SW1P 4DF

The Prime Minister
The Rt. Hon. David Cameron MP
10, Downing Street
London
SW1A 2AH

11th January, 2011

Dear Prime Minister,

You wrote to me on 14th October 2010, requesting that I reported to you, the Home Secretary (in relation to the Security Service) and the Foreign Secretary (in relation to SIS and GCHQ) before the end of 2010 on the adequacy of policies and procedures in the agencies, and a proposed framework for ongoing oversight by the Intelligence Services Commissioner, in respect of the acquisition, retention and deletion of bulk personal data holdings and in respect of the access to and use of such data.

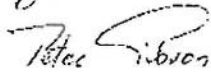
To that end, I have had meetings with the three agencies to review their existing policies and internal procedures and I have paid trial inspection visits to each agency to work out with that agency the most effective method of conducting oversight in accordance with agreed principles. All the agencies have cooperated to the fullest possible extent. It has been of very great assistance to me that I have been accompanied on those visits by Sir Mark Waller. The agencies have thus had the benefit of receiving his preliminary views as well as hearing my comments.

My accompanying report reflects what I have found on my review of the agencies' policies and procedures and the framework agreed with the agencies for the oversight by the Intelligence Service Commissioner of those policies and procedures in the light of my trial inspection visits.

39

When on 22nd October 2010 I responded to your letter I said that I would do my best to report to you, the Home Secretary and the Foreign Secretary before the end of 2010 as requested. Unfortunately, it has proved impossible to adhere precisely to that timetable. I apologise for the resulting small slippage which I hope has not inconvenienced you.

Yours sincerely,

A handwritten signature in black ink that reads "Peter Gibson". The signature is written in a cursive style with a large, sweeping initial "P".

The Rt. Hon. Sir Peter Gibson