[redacted]

Report of Sir Peter Gibson on the bulk personal data holdings of the Security Service, SIS and GCHQ

1. Each of the three security and intelligence agencies (" the SIA") holds copies of bulk personal datasets, that is to say datasets acquired under s. 2 (2)(a) Security Service Act 1989 ("SSA") or ss. 2(2)(a) or 4(2)(a) Intelligence Services Act 1994 ("ISA") which contain data about a wide range of individuals, including data about individuals who are not of direct intelligence interest. Most of that data is focused on 'nominal' data, such as a name, date of birth and an address, sometimes with additional information about foreign travel [redacted] e.g. passport number [redacted] The data has been characterised for the most part as being broad, in that it refers to numerous real people, but shallow in that it contains no information about such things as health [redacted]

2. Each agency is aware that it can only acquire, retain and exploit such data when to do so is necessary for the proper discharge of its functions in accordance with SSA or ISA as the case may be. Its procedures comply with that basic requirement. Each agency has also geared its procedures to be in conformity with other legislation which affects it. For example, in all its actions related to such data that has been acquired under the Regulation of Investigatory Powers Act 2000 ('RIPA'), it has to satisfy the RIPA tests of necessity and proportionality. Each agency's procedures have regard to the applicable principles of the Human Rights Act 1998. Accordingly the level of intrusion must be justifiable under Art. 8 (2) of the European Convention on Human Rights. Each agency's procedures also have regard to the Data Protection Act 1998 ("DPA"), which requires that personal data should be processed fairly and lawfully, obtained only for specified purposes, not be further processed in any manner incompatible with those purposes and kept no longer than necessary. It seeks to comply with DPA principles, wherever

[redacted]

possible within operational constraints, and where that is not possible, s.28 provides an exemption for national security. All three agencies have obtained Ministerial certificates which provide conclusive evidence that the national security exemption is required in respect of personal data obtained and processed in performance of their statutory functions. The agencies only deploy the certificates on a case-by-case basis where it is necessary to do so.

3. The justification for the acquisition, retention and exploitation by an agency of the bulk personal datasets lies in the context in which the SIA operate. They face increasingly sophisticated and diverse challenges in their work to counter terrorism and other threats to the UK's national security and economic well-being. They now have many more potentially serious but sketchy leads on targets who are more mobile and have access to capability-boosting technologies. To tackle this effectively the SIA need to be able quickly to identify and track individual targets and target networks, including ones in which the majority of members may be unknown and on which there is little intelligence. To ensure that significant threats are identified quickly they need to be able to cover more cases quickly from initial lead to closure. Further, they need to be equally competent in making connections in support of work to obtain high quality secret intelligence and to counter threats in other areas, such as counter proliferation.

4. The SIA say, in my opinion justifiably, that without the bulk personal data now available to them they could not offer the same level of assurance. If they could no longer exploit to the maximum this data, and the analytical and investigative capabilities developed around it, they could not be confident of producing timely intelligence from partial information and clues. The covert nature of their work, the large number of terrorist targets, the need to be able to detect new targets on the basis of known or emerging target behaviour, the fragmentary nature of many intelligence leads and the magnitude of the threat all mean that without the appropriate use of bulk personal data there would be no effective methods for resolving identities in a timely fashion.

[redacted]

5. For the analytical and investigative techniques to work, the SIA require substantial volumes of data. The vast majority of this data relates to people who are not of security or intelligence interest. It is only through targeted searching and data manipulation that relevant data is isolated and acted upon. The nature of the challenge means that it is not possible to anticipate what will be of direct value as new targets emerge all the time.

6. Each agency is properly aware that a significant responsibility is placed on it to ensure that its privileged access is not misused. During data analysis, intelligence officers manipulate data associated with large numbers of individuals. Such are the size and format of these datasets that the datasets used in this way are effectively anonymised by volume and sometimes by the way in which the data is structured. It is more accurate generally to refer to analysts being able to submit structured queries which will access and retrieve potentially relevant personal data rather than their having direct access to row upon row of such data. Some analysis may necessarily in its early stages result in retrieval of data about individuals of no intelligence interest, but an objective of the analysts is to filter out records of individuals not linked to the investigation at the earliest possible stage in order to permit the focus to be concentrated on the true intelligence target. The agencies apply management and security audit processes to reinforce this discipline.

7. Although the agencies have different remits and methods of working, they have comparable procedures aimed at ensuring that they

- acquire only the data which they need to perform their legitimate functions with due regard to necessity and proportionality and in accordance with the law;
- consider the intrusiveness of individual datasets before seeking to acquire them and before sharing them with others;
- take appropriate measures to restrict access to this data to those performing legitimate and necessary enquiries, with suitable management and security audits;

43

[redacted]

- share data, either across the SIA or with other partners, only when it is necessary and proportionate to do so;
- hold data only for as long as it is necessary; and
- apply suitable levels of oversight to all stages of the data life cycle.

Security Service

8. [redacted]

9. For the acquisition of a dataset, the Security Service investigative desk must make a written case to senior management that the acquisition is necessary and proportionate. The matters considered will include whether it is logistically possible to exploit the data, if acquired, whether there are any less intrusive means and whether the data is particularly intrusive with respect to individual privacy. If the case is approved, a separate team is charged with negotiating the data acquisition. [redacted] The Security Service has to demonstrate to the data owner that the

44

[redacted]

intended use of the data is proportionate and that safeguards against misuse are in place. [redacted] This is intended to ensure that it only acquires data necessary to enable it to carry out its functions. [redacted]

10. Around [redacted] in the Security Service are able to interrogate its bulk personal data holdings. They are first trained to understand the appropriate and proportionate use of such techniques and must sign a code of conduct for lawful use. Each time users log onto the Security Service's database, they are made aware that unauthorised access is a criminal offence. The Security Service regularly audits the use of its intelligence systems and routinely conducts interviews with users to confirm that searches were appropriate. It does not speculatively search its bulk personal data holdings against generic target profiles. Almost without exception it only searches such holdings in response to specific intelligence in order to identify or acquire further information on real, although not necessarily fully identified, targets.

11. All bulk personal datasets are reviewed on a regular basis to determine whether they should be retained or deleted. The Security Service has a bulk data review board which meets every 6 months and comprises senior representatives of its legal and investigative branch and its internal ethics counsellor. When considering whether a dataset should be retained or deleted, the board considers how often the dataset has been used, whether it is obsolete and how easy it would be to update the data. Minutes are kept of the review board meetings and all deletions actions are logged.

12. The Security Service has a policy document covering the bulk personal data life cycle from acquisition to use to deletion. It is available to all staff. Its management board looks at its work on bulk data in the broader context of information policy on an annual basis.

[redacted]

SIS

13. SIS currently holds [redacted] datasets which are available to be searched by analysts through its bulk data exploitation tool, [redacted] Its holdings include UK Government owned datasets ([redacted] datasets commercially acquired and datasets covertly acquired. Such datasets are predominantly related to overseas activities and travel but include UK citizens and individuals based in the UK.

14. As with other SIS operations, it seeks authorisation from the Secretary of State for politically sensitive data acquisitions as appropriate. Otherwise, authorisation is given at senior official level and legal advisers are consulted as and when necessary. In seeking internal authorisations, officers must justify why acquisition and/or exploitation of the dataset is necessary in terms of fulfilling SIS's statutory functions, how it will be used, whether the results can be obtained by other means, and must include an assessment of the level of intrusion into personal privacy involved, for example whether it includes particularly sensitive personal information. Officers must also indicate how long they expect the data to be retained. Personal data stored within SIS's bulk personal data holdings are not recorded on its files or personal indices unless the subject has been identified through activity or associations as a legitimate subject of interest.

15. [redacted] officers are trained and authorised to perform standard searches. A much smaller number of officers undertake more extensive training to perform more complex enquiries. SIS does not require its officers to enter the reason for a search before the database can be accessed. However, a general warning appears when the officer logs on and this highlights the controlled use of the system and the monitoring which takes place. All users are required to accept the security operating procedures. An audit of use is conducted by a team separate from that conducting the query in order to identify and investigate unusual or inappropriate searches. SIS mainly uses its

[redacted]

database to acquire additional personal information on existing targets rather than using pattern analysis to develop new targets. For this reason it believes that the extent of collateral intrusion is small.

16. A team of senior SIS officials including legal advisers reviews database holdings usually every 6 months. The team uses quantitative and qualitative indicators to judge the database holding's ongoing usefulness and proportionality. It considers questions such as how up-to-date the data is, how often the database has been used and with what outcome, how sensitive the holding is both in terms of the degree of intrusion into privacy and potential exposure to SIS and how hard it would be to replace the data if the holding was deleted. This exercise has resulted in a number of deletions of datasets from [redacted] SIS holds some datasets off-line until it is certain that they will not be required in future.

17. SIS has published a formal statement of its policy on acquiring, exploiting and retaining bulk personal datasets to provide guidance to staff on the legal framework and policy principles involved and the measures taken to ensure proper use and accountability.

GCHQ

18. GCHQ has acquired and holds [redacted] bulk personal datasets. [redacted] The others generally have an overseas focus and are related to communications, travel or finance. The overwhelming majority of the non-targeted bulk data held by GCHQ is communications-related metadata intercepted under RIPA warrants and overseen by the Interception of Communications Commissioner. A lesser amount of untargeted bulk communications metadata is provided to GCHQ by Communications Service Providers under directions issued by the Secretary of State in accordance with the Telecommunications Act 1984. Very little of all this metadata is bulk personal data within the meaning given in paragraph 1 of this report.

[redacted]

19. As a matter of policy GCHQ applies the statutory safeguards under RIPA to all of the data which it holds. Managers are made aware of their responsibility to ensure the necessity and proportionality of any data acquisition or handling through personal letters of delegation. The GCHQ Compliance Guide makes specific reference to non-targeted bulk personal data and sets out procedures for how this data should be handled. GCHQ has a formal process for authorising the acquisition of personal data from external sources. This process addresses the necessity and proportionality of such acquisition with direct reference to its intrusiveness and sensitivity and only three officers in GCHQ's central policy unit can give approval for this acquisition.

20. GCHQ uses access to non-targeted bulk personal and communications metadata to provide further information on targeted communications addresses. Bulk communications metadata can be used to identify communications events or addresses for possible further investigation through association with known targets or profile-matching. These events and addresses remain anonymous until such time as they are identified with a high degree of certainty as being associated with a known or likely intelligence target. This provides an additional level of reassurance that analysts are only accessing personal data pertaining to known or suspected targets. Further, to perform any database query an analyst is required (by a 'pop-up' justification screen) to input (i) the purpose of the query which must fall within the statutorily authorised purposes, (ii) the JIC requirement number and (iii) the explanation for the query. These justifications are intended to satisfy HRA requirements for potentially intrusive actions. They are subject to audit on a sampled basis. GCHQ informs me that it is also in the process of extending security audit to all its non-targeted bulk personal datasets in order to detect potentially suspicious access.

21. GCHQ's data retention policy sets out the maximum periods for which the various types of information acquired and held by GCHQ can be retained and the intervals before that retention will be reviewed. Where a bulk dataset contains non-targeted personal data, its continued retention is reviewed

[redacted]

periodically by a panel of senior officials who also review how the data is accessed and the number of analysts having access. Where the case for retention is made out, the dataset will not be reviewed for another 12 months. If the case is less clear, it will be reviewed after 6 months or the data will be deleted.

22. At GCHQ I was also briefed on its holdings and use of bulk communications data acquired directly from Communications Service Providers with Directions issued by the Secretary of State (in practice to date, previous Foreign Secretaries) under Section 94 of the Telecommunications Act 1984. This is not 'personal' data in the sense that it contains names or other personal attributes beyond, typically, a telephone number. However, although there is a statutory basis for the acquisition of such data in this way, there is no statutory basis for independent oversight. As with bulk personal data, it would be desirable to rectify this situation when the opportunity presents itself. GCHQ requested before my visit that in the meantime the Commissioner should also review this subject on an informal basis. I was able to learn how GCHQ uses such Directions and how its analysts handle and exploit one dataset which I had pre-selected from a short menu. On the basis of this limited sample, I was satisfied that GCHQ was able to demonstrate the necessity of holding this data, that it obtains good and unique intelligence from it, and that its handling of the data is proportionate.

Conclusion

23. In recent years, each agency has developed its policy and practices relating to the management of bulk personal dataset holdings as such data has become more central to its work. Given the agencies' individual remits and working methods there are differences between each agency's detailed policies, mechanisms and management of user behaviour. These are tailored to each agency's statutory functions and operational methodology. Thus, GCHQ's 'pop up' justification screen was introduced some years ago as part of a RIPA compliance arrangement. Within the Security Service the bulk data is searched through the same mechanism as that which enables intelligence

[redacted]

material to be searched. The Security Service's approach to compliance considerably predates the beginning of bulk data analysis. In recent years the development of bulk data capabilities has been one driver for the strengthening of compliance arrangements. But in such arrangements emphasis is placed on personal and managerial responsibility and on a visible compliance audit.

24. There has been mutual visibility between the agencies and sharing of best practices. All three agencies have sound policies, internal processes and practices in place to ensure that data users comply with, and in some cases exceed, the requirements of the relevant human rights and data protection legislation and to minimise the risk of data being misused. These processes properly recognise the potentially intrusive nature of bulk personal data and, in my opinion, comply with the legal requirement on each agency to ensure that it is both necessary and proportionate for the agency to acquire the data, that the agency retains the data for only such time as the retention is necessary and proportionate, and that such data is accessed only by vetted staff with a genuine business need to do so.

Oversight by the Intelligence Services Commissioner

25. With the agreement of the SIA, the Commissioner will pay an inspection visit to each agency every half year. It is intended that such visits will be an extension of the half-yearly visits carried out by the Commissioner in the performance of his statutory duty of review. Similar practices will prevail. Thus each agency will provide the Commissioner with a list of all the bulk personal datasets held at the time of the visit and of all reviews and deletions since the last visit by the Commissioner. SIS will include in its list all datasets held off-line. The Commissioner will be free to choose which holdings he wishes to inspect in greater detail on his visit. It will keep him informed of any changes in its policies and procedures in relation to bulk personal data and it will promptly draw to his attention any failure, which comes to its notice, to comply with those policies and procedures. The agency will provide him with all the information and documentation on bulk personal

50