*All gists in the following extract have been double-underlined

User Comms 2011 - 2014

SIS Notice to all staff 2 October 2009

SERVICE POLICY ON COLLECTION & EXPLOITATION OF BULK DATA

Summary

Announcement of SIS policy on acquisition and use of bulk data; background to bulk data and its use, including legal foundations.

Detail

What is bulk data?

1. Like Security Service and GCHQ, SIS collects large volumes of bulk data. We are working to develop a tri-Agency common definition, but for SIS purposes we currently define bulk data as "raw electronic information on multiple individuals or organisations, which may contain the details of untargeted individuals and which is sought or processed for intelligence purposes".

2. Bulk data is a comparatively new and increasingly valuable category of intelligence source material. Each agency uses it slightly differently. We exploit this data to support current operations and to develop new ones. [redacted]

How do we use bulk data?

3. Bulk data exploitation can be a very powerful tool, enabling us to search across multiple data sources (eg [redacted], travel, financial and telecommunications) and to identify connections between individuals. Because it may include information on untargeted individuals [redacted] it is also potentially more intrusive than traditional and targeted information. We balance this intrusiveness by the way in which we hold, store and use the data, taking into account our obligations under the Intelligence Services Act and other relevant legislation.

4. A name or other identifying detail contained within a data set is only revealed by a search for that detail, or for someone or something associated with it. And, as with other SIS records, we may only search for and access information for legitimate reasons. We are also sensitive to valid concerns about the necessity and proportionality of holding large data sets and appreciate the current public debate around this issue. We have worked hard to develop a sound framework for this work and this is set out below. Our – and SIA partners' - arrangements are also currently being reviewed by the Cabinet Office and we welcome this external scrutiny.

Service policy

5. We have now formalised Service policy on the acquisition, exploitation and retention of bulk data. The policy (which will be added to SIS policy guidance in due course) is attached and covers:

- **Statement of Purpose and Definition** – what bulk data is and why we collect it.
- **Co-ordination** – the relevant team's role as the Service's bulk data capture & exploitation lead.
- **Legal Framework –** the Service's obligations under the Human Rights, Intelligence Services and Data Protection Acts.
- **Service Policy** – Service approach to the various categories of data, including the submissions process and the ways in which the Service mitigates the intrusiveness of bulk data capture and exploitation.
- **Data Acquisition and Transformation:** Data Ownership and mandatory practices.
- **Exploitation and Reporting -** responsibilities for action-on, recording of outcomes.
- **Data Sharing:** procedures and rules for sharing, with GCHQ/Security Service (including joint operations) and with OGDs/liaison
- **Data Review -** procedures to meet legal obligations on retention of bulk data
- **Data Security and Media Storage** - procedures for retaining original media and security standards.

6. If you have any questions please contact the relevant teams, or consult the database user guide on the intranet.
[Attached: Bulk Data Policy v1]

SIS Notice to all staff 5 November 2010

SIS POLICY ON ACQUIRING, EXPLOITING AND RETAINING BULK PERSONAL DATA

Summary:

- The Service continues to audit data systems such as the database to detect and prevent inappropriate or illegal use
- The Service's policy on bulk data has been updated include SIA coordination and oversight arrangements, and can be read here.

Detail:

We remind all database users that it, like other SIS data systems, may only be searched for official business reasons. Misuse of information in the database, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence.

The policy explains the potential intrusiveness of the datasets held and the various ways in which the Service mitigates this (whilst permitting database users to search across all datasets).

Through a variety of means the Service audits and monitors use of its IT systems to detect and prevent inappropriate or illegal use, to ensure and maintain the effective use of the systems, and for protective security reasons. Unusual activity on the database that gives rise to security concerns will be investigated and users may be asked to explain their use of the system.

More Information

- The Service's policy on bulk data (first published in Notice to all staff of 2 October 2009) [LINK]
- Full guidance on using the database is available on the intranet (see the database tab under 'How do I'). [LINK]

[Attached: Bulk Data Policy v2]

11 April 2011 – The database Code of Practice revised and version 2 placed on the intranet.

9 June 2011 – Log-On screen on the database revised (reminding users of Security Department and Intelligence Services Commissioner scrutiny and that misuse can represent a criminal offence and lead to disciplinary action).

Database Newsletter of 8 September 2011

SIS database - 'Do's and don'ts'

We've seen a few instances recently of individual users crossing the line with their database use for instance, looking up addresses in order to send birthday cards, checking passport details to organise personal travel, checking details of family members for personal reasons. Another area of concern is the use of the database as 'convenient' way to check the personal details of colleagues when filling out Service forms on their behalf.

Please remember that every search has the potential to invade the privacy of individuals, including the privacy of individuals who are not the main subject of your search, so please make sure you always have a business need to conduct that search and that the search is proportionate to the level of intrusion involved. In such instances it's much better to rely on less intrusive ways of obtaining the information eg. ensuring you have Section records containing staff members' address and passport details or simply waiting to obtain the details from the individual or another colleague.

We think it's worth a reminder about your responsibilities when using the database.

DO

*- Ensure you are compliant with the database Code of Practice - **(click here)***
*- Ensure that any use of the database is **necessary, proportionate and relevant to your job function***
- Report any accidental viewing/searching to a member of the security team.

DON'T

- Search for individuals for which you have no business need to do so (eg. public figures, family members)
- Share your credentials or allow others access via your credentials
*- Conduct searches on behalf of a colleague unless satisfied there is a business need for **you** to do so (it is you who will be asked to account for your search)*
- Share data from the database in a way that is not necessary, proportionate, within the remit of the Service and appropriate to your current role and responsibilities.

The list above is not exhaustive so please do familiarise yourself with the Code of Practice, which we are about to re-issue to all users. If you have any questions on any of the above the relevant team will be more than happy to answer them [redacted].

23 November 2011 – The database Code of Practice was issued to all users who were required to sign and return.

Notice to all staff 24 November 2011

MISUSE OF SIS BULK DATA

Summary

•All users given access to SIS systems should search data only when they are satisfied it is necessary and proportionate to do so, and in support of the Service's statutory functions;
•Deliberate or serious abuse of SIS systems could amount to gross misconduct and may result in dismissal.

Detail

The exploitation of bulk data is critical to many SIS operations, delivering real value to teams and driving forward new ways of working. But this capability must be used responsibly.

There have been several recent instances of data misuse. These have resulted in disciplinary action and in one instance a contract was terminated.

By its nature, bulk data includes personal information on large numbers of individuals not of intelligence interest. In acquiring and exploiting this data, SIS works within the legal framework of the Intelligence Services, Data Protection and Human Rights Acts. All staff, secondees and contractors are required to adhere to SIS's Bulk Data Policy. This includes measures to safeguard the privacy of the individuals whose data the Service holds. It requires that those given access to the data search it only when they are satisfied it is necessary and proportionate to do so, and in support of the Service's statutory functions.

Officers are required to exercise their judgement in determining whether their searches meet this threshold and may be asked to justify searches to their Line Management or to the Intelligence Services Commissioner, who regularly scrutinises the Service's disclosure arrangements.

Misuse of Service databases, including unjustified access, is unlawful and could constitute a criminal offence.

Any misuse of data will be investigated and may result in disciplinary proceedings. Deliberate or serious abuse could amount to gross misconduct and may result in dismissal or, for secondees, contractors and consultants, termination of contract.

If you are unsure about whether or not searches meet these criteria, please seek guidance from the relevant team. You should also familiarise yourself with the database searches that would not meet these criteria and the Do and Don't guidance given below.

Dos and Don'ts

- Do not search for and/or access information other than that which is necessary and proportionate for your current work.
- Do be prepared to justify any search that you undertake on Service databases.
- Do structure and target your queries on databases in a way that is most likely to retrieve information that is relevant to your enquiry.
- Do raise any concerns that you may have about how others are using Service databases, either with your line manager or with a security officer.
- Do report any error in searching Service databases, to a member of the security section by email, explaining the circumstances. For example e.g. an incorrect search.
- Do not attempt to access Service databases by any means other than your allocated credentials.
- Do not share your credentials with another individual.

SIS Database Newsletter of 1 December 2011

SIS Database Usage Reminder

All users should be aware of the guidance for using the database so that your searches are necessary and proportionate and in support of the Service's statutory functions. Please ensure you have read the recent notice to all staff (24 November 2011) on bulk data and associated Bulk Data Policy. There are also Hints and Tips on necessary and proportionate searching in the database linked to the notice to all staff, but if you have any questions, please don't hesitate to contact the relevant team.

Please also remember that it is vital that you request Action On for database data or [redacted] analysis if this information will be sent/used outside of SIS, Security Service or GCHQ. The Security Service and GCHQ should also revert if they wish to use SIS bulk data more widely. Again, please contact the relevant team if you have any questions.

The database Newsletter of April 2012

The database Code Of Practice update
We are aware that of some concerns amongst database users as to what officers can and cannot search for on the database. As each individual search tends to be unique it is difficult to provide definitive guidance however the best principle to work on is to always make sure you have a valid ***business reason*** *for every search. We recommend users keep some record (eg. a personal message, email or diary note) for each search they carry out - this will ensure that you are able to justify the necessity and proportionality of any search, whether for audit purposes or scrutiny by the Intelligence Services Commissioner. If you have any doubts about carrying out a search then call a senior SIS official who is happy to provide guidance on a case by case basis.*

Unused accounts to be disabled
Due to the intrusive nature of database data it is vital that we can prove that only those with a continuing business need have access to the system. As announced in a previous notice to all staff we are now operating a policy of automatically disabling database accounts that are not used within the last six months. Access can be restored through re-application.