GISTS SHOWING IN UNDERLINED AND ITALICS

Witness: *MI5 WITNESS*
Party: 4th Respondent
Number: 1
Exhibit: *MI5* 2
Date: 10.2.17

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

WITNESS STATEMENT OF *MI5 WITNESS*

I, *MI5 WITNESS*, Deputy Director in the Security Service, of Thames House London SW1, WILL SAY as follows:

1) *I am responsible, amongst other things, for the data governance team.*

2) I am authorised to make this statement on behalf of MI5. 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 MI5.

3) Exhibited to this witness statement is a bundle of documentation marked "*MI5* 2". References in this statement to page numbers (eg [pages xx to xx]) are to the page numbers of *MI5* 2 (page numbering is in the top right hand corner of each page).

agreed. *I am unable to confirm or deny in this OPEN statement whether any agreement to such sharing with foreign liaison partners or LEAs has been given over this period.* I have no reason to believe that any sharing of BPD would have taken place without appropriate authorisation.

Sharing of BCD with international partners and LEAs

9) The sharing of MI5's BCD (ie [REDACTION]) or a sub-set of that BCD (itself amounting to bulk communications data) would require the approval of the Home Secretary or a Senior Official in the Home Office (paragraph 4.4.1 at page 12). *Any sharing request would have to be dealt with in the data governance team, and I have made inquiries as to whether the agreement of the Home Secretary (or the Home Office) has been sought to share its BCD, or a sub-set of its BCD, with either international partners or LEAs. I am unable to confirm or deny in this OPEN statement whether any agreement to such sharing has been sought over this period in relation to foreign liaison partners or LEAs. I have no reason to believe that any sharing of BCD would have taken place without appropriate authorisation.*

10) *Whilst I can neither confirm nor deny whether MI5 has agreed to share or in fact shares BPD/BCD with either foreign liaison or LEA, were we to do so, we would:*

a) *follow the principles and approach set out in our Handling Arrangements and policy/guidance;*
b) *take into account the nature of the BPD and BCD that was due to be disclosed;*
c) *take into account the nature/remit of the body to which we were considering disclosing the BPD/BCD;*
d) *take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed.*

Statement of Truth

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

MI5 Witness

Dated: 10 Feb 17

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

which it is hosted. These safeguards include (but are not limited to) audits, protective monitoring regimes, line management oversight, training and codes of practice;

- The Agencies will take appropriate disciplinary action against any person identified as abusing or misusing analytical capabilities, BPD, or any information or intelligence derived therefrom.

15. These policy statements apply SIA-wide. Each Agency maintains separate complementary policy and guidance to aid staff in the use of BPD and meeting these policy requirements.

D. Sharing

16. All three Agencies have a common interest in acquiring and interrogating BPD. As a principle, all three Agencies will seek to acquire once and use many times, on grounds of business effectiveness and efficiency. The following policy statements apply to the Agencies:

- When sharing BPD the supplying Agency must be satisfied that it is necessary and proportionate to share the data with the other Agency/Agencies; and the receiving Agency/Agencies must be satisfied that it is necessary and proportionate to acquire the data in question. A log of data sharing will be maintained by each agency;
- The sharing of BPD must be authorised in advance by a senior individual within each Agency, and no action to share may be taken without such authorisation;
- [REDACTION]
- BPD must not be shared with non-SIA third parties without prior agreement from the acquiring Agency;
- *Were BPD to be shared with overseas liaison the relevant necessity and proportionality tests for onwards disclosure under the SSA or ISA would have to be met. In the event that one (UK) Agency wished to disclose externally a dataset originally acquired by another Agency, Action-On would have to be sought in advance from the acquiring Agency. Wider legal, political and operational risks would also have to be considered, as appropriate.*
- The Agencies may share applications (which in turn could provide access to another Agency's BPD holdings) as judged appropriate in line with SIA *information policy* on commissioning.

17. These policy statements apply SIA-wide. Each Agency maintains separate complementary policy and guidance to aid staff in the process of sharing BPD and meeting these policy requirements.

E. Retention

18. The Agencies review the necessity and proportionality of the continued retention of BPD. The following policy statements apply to the Agencies:

- Each Agency has a review panel which will review BPD retention by that Agency. In all three Agencies, panels sit once every six months;
- These panels will invite representatives from each of the other Agencies to discuss data sharing (both data and applications granting access to BPD), assist consistency of decision making across Agencies, and provide inter-Agency feedback;

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

Sharing Bulk Personal Data

The sharing of BPD is carefully managed to ensure that disclosure only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside the Security Service rests with *a senior MI5 official* on behalf of DSIRO.

Sharing within the SIA

To the extent the SIA all have a common interest in acquiring information for national security purposes, it may be lawful for MI5 to share BPD with SIS or GCHQ. Within the SIA, the relevant gateways for these purposes are (i) section 2(2)(a) so far as disclosure by the Security Service is concerned, and (ii) sections 2(2)(a) and 4(2)(a) respectively of Intelligence Services Act so far as acquisition by SIS and GCHQ are concerned.

In relation to each dataset, there are two sides to the information transaction, whereby both the disclosing and receiving agency have to be satisfied as to the necessity and proportionality of sharing a particular dataset. MI5 need to establish in each case that both (i) disclosure by the Security Service under section 2(2)(a) is necessary for the proper discharge of the Security Service's statutory function of protecting national security, and also (ii) that acquisition by SIS and GCHQ is necessary for their respective statutory functions in respect of national security under sections 2(2)(a) and 4(2)(a) respectively of ISA.

In circumstances where GCHQ or SIS identifies a requirement, they should discuss their requirements with the relevant MI5 data sponsor. If the requesting agency and the MI5 data sponsor believe there is a business case to share the data a formal request must be made to MI5 via *a relevant form*. [REDACTION] The relevant data sponsor is then responsible for submitting *the relevant form*.

The relevant form.

The relevant form outlines the business case submitted by the requesting Agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements. This must be approved by the relevant data sponsoring *senior MI5 official* before being submitted to *the relevant team* who will consult *a legal adviser* on the legality of disclosure and the relevant technical feasibility.

A senior MI5 official will confirm the strength of the business case for sharing data is sufficient, and any security, ethical and reputational risks have been adequately considered. [REDACTION]

Once *the relevant form* is approved by *a senior MI5 official*, arrangements will be made for the data to be shared with the relevant Agency using suitably accredited network for electronic transfer. Where electronic transfer is not possible, physical transfer must be conducted in accordance with policy.

Sharing data and applications in-situ

[REDACTION] Sharing data in this way requires both the requesting and disclosing agencies to assess the necessity and proportionality of the access and use being sought [REDACTION

The senior MI5 official should be consulted in relation to any proposals to access data on other SIA systems, or to allow SIA access into MI5 systems.

Sharing outside the SIA

MI5 neither confirms, nor denies the existence of specific BPD holdings to organisations outside the SIA or a limited number of individuals within OSCT. Therefore any request to share BPD with an organisation other than GCHQ or SIS should reiterate this position as the requestor should approach the provider themselves. Attempts to ascertain MI5 BPD holdings by non-SIA organisations should be reported to *the relevant team*.

6

[REDACTION]

(5)

including in particular what intelligence aim is likely to be met and how the data will support that objective.

- **The proportionality of acquiring and retaining the data, including in particular whether there is a less intrusive method of obtaining the data.**

When seeking authorisation to load a BPD into an analytical system for use, staff must satisfy themselves as to, and explain:

- **The purpose for which the BPD is required; and**
- **The necessity and proportionality of using the BPD.**

5.0 Specific Procedures and Safeguards for Use of and Access to Bulk Personal Datasets inside each Intelligence Service

5.1 Each Intelligence Service attaches the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. In particular, each Intelligence Service must apply the following protective security measures:

- Physical security to protect any premises where the information may be accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

5.2 In relation to information in bulk personal datasets held, each Intelligence Service is obliged to put in place the following additional measures:

- Access to the information contained within the bulk personal datasets must be strictly limited to those with an appropriate business requirement to use these data;
- Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service;
- If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, they must only access the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Service, or for the additional limited purposes described in paragraph 3.1.4 above;
- Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate (as described in paragraphs 4.4 above and 6.3 below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;

policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State.

When seeking to disclose the whole (or a subset) of a BPD, staff must be satisfied that disclosure is:

- **Justified on the basis of the relevant statutory disclosure gateway.**
- **Determined to be necessary and proportionate to the objective.**
- **Limited to only as much information as will achieve the objective.**
- **Authorised by a senior manager or, in difficult case, the Secretary of State.**

7.0 Review of Retention and Deletion

7.1 Each Intelligence Service must regularly review the operational and legal justification for its **continued retention and use** of each bulk personal dataset. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Intelligence Service must be deleted or destroyed.

7.2 The retention and review process requires consideration of the following factors:

- The operational and legal justification for continued retention, including its necessity and proportionality;
- Whether such information could be obtained elsewhere through less intrusive means;
- An assessment of the value and examples of use;
- Frequency of acquisition;
- The level of intrusion into privacy;
- The extent of political, corporate, or reputational risk;
- Whether any caveats or restrictions should be applied to continued retention.

For the purposes of retention, review and deletion of BPD-sets, each Intelligence Service must:

- **Regularly review the justification for continued retention and use, including its necessity and proportionality.**
- **Delete a BPD after a decision is made that retention or use of it is no longer necessary or proportionate.**

8.0 Other management controls within the Intelligence Services

8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Service by an Internal Review Panel, whose function is to ensure that each bulk personal dataset has been properly acquired, that any disclosure is properly justified, that its retention remains necessary for the proper

OPEN version of page (9)

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

6.2.6 The ***relevant form*** outlines the business case submitted by the requesting Agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements. Disclosure of the whole BPD (or subset thereof) is only permitted once such authorisation has been given under this process. Once the authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring Agency.

6.3 Disclosure to liaison services

6.3.1 [REDACTION]

6.3.2 There are however some circumstances, such as a pressing operational requirement, where disclosure to a liaison service [REDACTION] may be necessary and proportionate in the interests of national security. In this event, the same legal disclosure tests would need to be applied as when disclosing to SIA partners, and ***the relevant form*** would have to be completed. MI5 would need to be satisfied that disclosure to the relevant liaison service met the dual tests of necessity and proportionality. All enquiries should be directed to ***the data governance team***. Prior to disclosure, staff must (a) take reasonable steps to ensure that the liaison partner has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data (including with regard to both source protection and the protection of the privacy of the individuals in the BPD) and ensuring that it is securely handled, or (b) have received satisfactory assurances from the liaison partner with respect to such arrangements.

Disclosure of MI5 BPD must be:

- **Justified on the basis of the relevant statutory disclosure gateway;**
- **Assessed to be necessary and proportionate to the objective;**
- **Limited to only as much information as will achieve the objective;**
- **Authorised *by a senior MI5 official* using *the relevant form*.**

7.0 DATA RETENTION AND REVIEW

7.1. Bulk Personal Data Review Panel

7.1.1 The Bulk Personal Data Review (BPDR) Panel currently meets at least every 6 months to conduct a review of bulk personal datasets in MI5's possession, to ensure that their retention and use remains necessary and proportionate for MI5 to carry out its statutory duty to protect National Security for the purposes of s.2(2)(a) Security Service Act 1989.

7.1.2 Panel members will satisfy themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR and is in line with the requirements of the Data Protection Act 1998. MI5 can only retain BPD where it is necessary and proportionate to do so, and if it is judged (at any time, but including on review) that it is no longer necessary and proportionate to retain a dataset, all copies must be deleted or destroyed.

7.1.3 ***The Panel consists of, amongst others, senior officials, Ethics Counsellor, non-executive director and legal advisor.***

communications data or of a subset of the bulk communications data rather than of the whole bulk communications dataset.

4.4.5 Before disclosing any BCD, staff must take reasonable steps to ensure that the intended recipient organisation has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled, or that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services and apply equally in making the decision to disclose an entire BCD, a subset of BCD, or an individual piece of data from the dataset.

Disclosure of BCD must be:

- **Justified on the basis of the relevant statutory disclosure gateway;**
- **Assessed to be necessary and proportionate to the objective;**
- **Limited to only as much information as will achieve the objective;**
- **Authorised by a Senior Official or Secretary of State (entire BCD or a subset).**

4.5 Review of Ongoing Acquisition and Retention, and Deletion

4.5.1 Each Intelligence Service must regularly review, i.e. at intervals of no less than six months, the operational and legal justification for its continued retention and use of BCD. This should be managed through a review panel comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

4.5.2 The retention and review process requires consideration of:

- An assessment of the value and use of the dataset during the period under review and in a historical context;
- the operational and legal justification for ongoing acquisition, continued retention, including its necessity and proportionality;
- The extent of use and specific examples to illustrate the benefits;
- The level of actual and collateral intrusion posed by retention and exploitation;
- The extent of corporate, legal, reputational or political risk;
- Whether such information could be acquired elsewhere through less intrusive means.

4.5.3 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State. In the event that the Intelligence Service or Secretary of State no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. The relevant Intelligence Service must then task the technical team[s] responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed and notify the Interception of Communications Commissioner accordingly. Confirmation of completed deletion must be recorded with the relevant Information Governance/Compliance team.

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

4.4.7 Where disclosure of an entire BCD (or a subset) is contemplated, (in addition to the requirement in 4.4.1 above) this is subject to prior internal authorisation procedures as well as to the requirements in 4.4.2-4.4.5 that apply to disclosure of individual pieces of data. Where these requirements are met, then (prior to submission to the Home Office/Home Secretary) the BCD is formally requested by the requesting agency from MI5 through an agreed sharing procedure using *the appropriate form*. *The data governance team* is then responsible for submitting *the appropriate form* seeking the approval of MI5's Director General. *The appropriate form* outlines the business case submitted by the requesting agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements

4.4.8 . If the Director General is content, a submission will be prepared for the Home Office and/or Home Secretary. Disclosure of the whole BCD (or subset thereof) is only permitted when this has been authorised by the Home Secretary or a Senior Official at the Home Office. Once authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring agency.

Disclosure of MI5 BCD must be:

- **Justified on the basis of the relevant statutory disclosure gateway;**
- **Assessed to be necessary and proportionate to the objective;**
- **Limited to only as much information as will achieve the objective;**
- **Agreed by DG and authorised by the Home Secretary or Senior Official (entire BCD or a subset).**

4.5 Data Retention, Review and Deletion

4.5.1 *The data governance team* is required to conduct a comprehensive review of the capability every 6 months on behalf of the BCD Governance Group (BCDGG), to ensure that retention and use remains necessary for the proper discharge by MI5 of its function of protecting national security under section 1 of the Security Service Act 1989 and is proportionate to the achievement of that objective. This review will include, but is not limited to:

- An assessment of the value and use of the dataset during the period under review and in a historical context;
- the operational and legal justification for continued retention, including its necessity and proportionality;
- The extent of use and specific examples to illustrate the benefits;
- The level of actual and collateral intrusion posed by retention and exploitation;
- The extent of corporate, legal, reputational or political risk;
- Whether such information could be acquired elsewhere through less intrusive means;
- Any relevant ethical issues;