Witness: SIS Witness
Party: 5th Respondent
Amended Number:2
Exhibit: SIS exhibit
Date: 03.03.2017

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 SIS WITNESS

I, SIS witness, of the Secret Intelligence Service (SIS), Vauxhall Cross, London, SE1, will say as follows:

1. [REDACTED] In my current role, I oversee the compliance of SIS operations with the law and other relevant guidance and directives. In that context, I attend the six monthly meetings of the Data Retention Review Board. I also have overall responsibility for SIS' engagement with oversight bodies, the Courts, Inquiries, Inquests, and Tribunals, including the Investigatory Powers Tribunal.

2. I am authorised to make this witness statement on behalf of SIS. 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 SIS.

3. Attached to this statement, and marked 'SIS exhibit' is a bundle of relevant documents. Save where otherwise stated, page numbers below refer to that exhibit.

4. This statement addresses the restrictions which would be placed were SIS to transfer Bulk Personal Datasets ("BPD") to foreign partners and/or UK LEAs since March 2015.

OVERVIEW OF SAFEGUARDS

5. In February 2015, a joint SIA BPD policy was agreed which set out the Agencies' policy in relation to Bulk Personal Data. It stated that "*each Agency must have arrangements in place for the effective management and legal compliance of BPD throughout its lifecycle.*" Specifically in relation to sharing, the policy stated the following:

"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 the 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;

Agencies must protect sensitive datasets (or certain fields within a dataset) when sharing, if the risk or intrusion in doing so is not judged to be necessary or proportionate;

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 dislose 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."

6. Open Handling Arrangements, which were published on 4 November 2015 and applied to the obtaining, use and disclosure of BPD, included details of procedures and safeguards for the disclosure of bulk personal data outside the relevant Intelligence Service. Paragraphs 5.2 and 8.1 detail the key safeguards, including access control, and state that any disclosure must be necessary and proportionate in accordance with SIS's statutory functions and purposes.

Paragraphs 6.0-6.7 set out the guidelines for the disclosure of BPD outside of SIS, including the need to consider whether to place restrictions when sharing BPD/sub-sets of BPDs, as follows:

"Before disclosing any bulk personal data, 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.

These conditions must be met for all disclosure, including between the Intelligence Services.

These conditions for disclosure apply equally to the disclosure of an entire bulk personal dataset, a subset of the dataset, or an individual piece of data from the dataset.

Disclosure of the whole (or a subset) of a bulk personal dataset is subject to internal authorisation procedures in addition to those that apply to an item of data. The authorisation process requires an application to a senior manager designated for the purpose, describing the dataset it is proposed to disclose

(in whole or in part) and setting out the operational and legal justification for the proposed disclosure along with the other information specified in paragraph 4.7, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so that the senior manager can then consider the factors in paragraph 6.1, with operational, legal and policy advice as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State."

7. In addition, the internal SIS Handling Arrangements came into force in November 2015, which included specific guidance to staff on the sharing of BPD with foreign partners, including the following:

"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 SIS rests with the senior SIS official."

8. The guidance also notes that:

"In the event that SIS deemed it was necessary and proportionate to disclose BPD to a liaison service, the same legal disclosure tests would need to be applied as when sharing with SIA partners. As part of SIS's analysis of whether disclosure is in line with its legal obligations, in the event that SIS shares BPD with a liaison service, SIS would require any such service to agree to rigorous requirements in relation to the safeguarding of that BPD. These safeguards would cover, amongst other things, access to the BPD, use (in terms of systems as well as purpose), and onward disclosure and will be set out on handling instructions that accompany each BPD.

The disclosure of BPD is carefully managed by the relevant team to ensure that disclosure only occurs when it is permitted under ISA 1994 and that clear necessity and proportionality cases are evidenced. Responsibility for disclosure of BPD rests with a senior SIS official in the relevant team."

SHARING WITH INTERNATIONAL PARTNERS AND LEAs

9. I am unable to confirm or deny in this OPEN statement whether there has been any agreement to share BPD with foreign liaison partners or LEAs since 11 March 2015.

10. Were SIS to share BPD with a partner it would consider any such proposal on a case by case basis, taking into account a number of factors.

    a. The nature of the partner with whom we are sharing. This includes considering the history we have of sharing intelligence with that partner; their data capability and practices; and their history of compliance, either where we have previously shared data or where we have shared actionable intelligence.

    b. The purpose for which it is envisaged BPD will be shared. This covers two considerations: firstly, the necessity case for SIS. At the highest level this means that there must be a requirement to share the BPD to assist SIS in meeting one of the four purposes for which information can be shared under section 2(2) ISA. Secondly, the purpose for which SIS understands that the recipient partner wishes to obtain BPD.

[REDACTED]

11. Should SIS decide that there was an 'in principle' argument for sharing, SIS would ensure that it had a sufficient understanding of the data handling regime in the recipient organisation to enable SIS to make a reasoned judgment as to whether disclosure was necessary and proportionate in the circumstances. As part of this 'due diligence' exercise, the following are likely to be relevant considerations: the anticipated benefit to SIS; the recipient partner's requirement to obtain BPD; and the nature and extent of any handling arrangements for BPD within the recipient partner organisation (in particular in relation to access, examination, storage and onward disclosure of the BPD and/or information derived from it). In addition, SIS would seek guidance from the recipient partner as to the legal provisions applicable in that partner's jurisdiction, including whether there were any legal obligations that were likely to prevent compliance with any restrictions that SIS would want/need to place on the use of the BPD. SIS's approach to this process would be informed by its existing knowledge of and relationship with the recipient partner (including knowledge and experience of their capabilities, intent and practice).

[REDACTED]

12. The due diligence exercise would seek answers to specific questions in relation to the governance and compliance arrangements of the recipient. This would provide SIS with the basis for assurance that they have in place equivalent standards as

would apply to SIS' own staff and procedures. The sorts of questions that SIS would seek satisfactory answers to in order to provide assurance of equivalent standards are likely to include (but not be limited to) the following areas:

a. Relevant questions of law and policy, for example, is the recipient organisation subject to provisions in law (international or domestic) that would govern their use of BPD? Are they governed by any statutory requirements that would tie their use of BPD to specific purposes? Are they subject to any legal obligations or policy commitments to protect the personal data or human rights of individuals?

b. Acquisition practices, for example, what factors would the recipient organisation take into account before acquiring BPD? Would necessity and proportionality be considered? Who would take part in the decision-making process and how would it be recorded?

c. Authorisation protocols, for example, what process would the recipient organisation apply to authorise the retention and exploitation of BPD? What would the criteria be that would be applied to establish that it is both necessary and proportionate to retain and use data? Would legal advice be obtained?

d. Data ingestion, for example, how would BPD be stored within a partner organisation? What would the system architecture be? What other data would be stored on the system or systems? What access control mechanisms would be in place for raw and processed data? Would access control be determined by role? Would specific training be provided (including in relation to legal/policy concerns) before access is granted to a system holding BPD? Are there categories that would be considered sensitive or privileged either by law or policy? Would ingestion of data of this type be subject to additional considerations? Would there be additional protections for data of this type at the point of access?

e. Use, for example, into which tool(s) within the recipient organisation would BPD be ingested? What would be the main purpose of the tool? What would a user be required to consider before searching within BPD? Would the user be required by law to think about the necessity and proportionality and/or the direct and collateral intrusion of conducting a search? How would such considerations be recorded? Would the tool limit the nature of extent of the search by a user? What safeguards would be in place to prevent misuse of BPD? Would user activity be subject to any auditing or monitoring? What would the consequences of an individual failure to comply with the law/policy on the use of BPD be? How

would SIS be notified of any failure to comply and what power would they have to dictate consequences?

f. Disclosure, for example, what safeguards would be in place within the recipient organisation to ensure Action On is obtained before any action, including the passing of information to a third party, is taken on information derived from BPD? Are there legal or policy requirements to ensure that the passing of any information would meet certain criteria? How would a user know that a particular piece of data requires Action On before they could use it? What would the process be for gaining Action On?

g. Retention and Review, for example, what process would be in place in the recipient organisation to review the necessity and proportionality for continuing to retain and exploit BPD? What would be the parameters for the review, and what criteria would be used to judge necessity and proportionality? What would the process be to delete data? What would the procedure be for deleting and destroying data?

h. Oversight, for example, what would be the internal and/or external oversight arrangements in place within the recipient organisation to audit the acquisition, retention and use of BPD?

13. Any such due diligence exercise would necessarily be bespoke and tailored to the potential recipient in question and the particular circumstances of the proposed sharing arrangement. The questions above are illustrative and neither exhaustive nor a proforma. In so far as possible, SIS would seek to validate answers given by means of 'in person' discussions with responsible officers of the recipient organisation and by reference to their internal policy documents, forms, codes of practice and training materials.

14. If a due diligence exercise did not result in the obtaining of satisfactory assurance, or if the veracity of answers obtained were in doubt, SIS would not share BPD. In any formalising written agreement SIS would set out the circumstances under which the arrangement could be halted if there was concern or evidence that arrangements were not satisfactory.

15. There are a number of ways in which a due diligence exercise might be pursued and could, for example, include a visit by SIS policy and legal staff to a potential recipient to observe and discuss their systems and processes. The process would be designed to ensure that SIS would have a comprehensive written record of the

way in which a recipient partner would handle BPD (covering all the matters set out in paragraph 12 above); as well as the domestic legal and compliance regime to which they would be required to adhere.

16. It is likely that any such due diligence exercise would be an iterative process. Supplementary questions may be required for clarification and to gain an accurate and complete picture of a potential recipient's compliance arrangements and to satisfy SIS's handling and compliance requirements.

17. Following a due diligence exercise, were SIS to still have outstanding concerns in respect of a potential recipient's data compliance, SIS would not share BPD.

18. Were SIS to be satisfied with a potential recipient's data compliance following a due diligence exercise, SIS would then proceed to set out and agree with the recipient partner the detail of the agreement to share. The detail of the agreement might vary with each individual recipient depending on the circumstances and the nature of SIS's relationship with them.

[REDACTED]

19. Were SIS to agree to share BPD with a particular recipient partner, the sharing of each subsequent dataset would be considered on an individual basis. Any decision to share would be subject to a formal and recorded decision-making process and would involve the input of a legal adviser where necessary. Considerations would include the necessity and proportionality case for sharing and how SIS think the recipient partner will use the data. SIS would also always consider whether the policy on Consolidated Guidance applies. The formal and recorded decision-making process would ensure that the approach to sharing outside of SIS is applied in a consistent manner.

20. SIS would ensure that dataset specific handling instructions would accompany any and each BPD shared.

21. The principal way in which compliance with the BPD handling instructions would be monitored is through the Action On process. This is the process whereby a customer requests permission to make active use of SIS intelligence. For instance Action On would include passing to a third party. The Action On process would be a crucial protection for ensuring that the recipient partner is adhering to the requirements agreed with it and set out in the handling instructions for each individual dataset.

22. Were SIS to not receive Action On requests where expected, this would be investigated.

[REDACTED]

23. In addition to the Action On process, SIS would conduct regular meetings, visits and discussions with any partners who might be in receipt of data sets. This would ensure that SIS's partners would be aware of changes to SIS's legal and compliance regime; and would enable SIS to obtain information about the changing technical, legal and compliance regimes of any partners. In that way, SIS would be able to assess on an ongoing basis whether the handling arrangements and other requirements that might apply to the sharing process remain fit for purpose.

24. Whilst we can neither confirm nor deny whether the SIA have agreed to share or in fact do share BPD with either foreign liaison or LEA, were we to do so, we would

- Follow the principles and approach set out in our respective Handling Arrangements and policy/guidance.

- Take into account the nature of the BPD that was due to be disclosed.

- Take into account the nature of the body to which we were considering disclosing the BPD.

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

.....SLS Witness.....

Dated: 3 March 2017