

Witness: SIS witness
Party: 1st and 2nd Defendants
Number: 1
Exhibit: []
Date: 04.02.2019

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

Claim No. CO/1052/2017

BETWEEN:

THE QUEEN
on the application of
LIBERTY

Claimant

-and-

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(2) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

Defendants

WITNESS STATEMENT OF SIS WITNESS

I, **SIS WITNESS A**, [Deputy Director in the Secret Intelligence Service], of [REDACTED]
[REDACTED] WILL SAY as follows:

1. In my current role, I oversee the compliance of Secret Intelligence Service (SIS) operations with the law and other relevant guidance and directives. This role includes overseeing the Service's response to disclosure requests related to inquiries such as this one. In this capacity, I provide assurance to C, the Service's Accounting

Officer, that we are effectively meeting our legal obligations. I am authorised to make this witness statement on behalf of SIS. The contents of this statement are true to the best of my knowledge and belief. Where matters are not within my direct experience, they are based upon documentation made available to me and discussions with others within SIS. This is the first witness statement that I have made in these proceedings. It should be read in conjunction with the statements provided by the Home Office, MI5 and GCHQ.

Use of Powers

2. The role of SIS, as set out in the ISA 1994, is to provide Her Majesty's Government with a global covert capability that facilitates the collection of secret intelligence and mount operations overseas to promote and defend the national security and economic wellbeing of the United Kingdom, and to prevent and detect serious crime. All SIS activity under the Investigatory Powers Act 2016 is related to those statutory functions. All SIS officers undergo mandatory compliance training and compliance is monitored by internal audit systems.

Arrangements under the Investigatory Powers Act 2016 ("the Act")

3. The Claimant in these proceedings is challenging powers in Parts 3, 4, 5, 6 and 7 of the Act, including powers for the Secretary of State or the Scottish Ministers to issue warrants under Parts 5, 6 and 7 of the Act to the Intelligence Services. Parts 5, 6 and 7 of the Act relate to targeted equipment interference, bulk interception, bulk acquisition of communications data, bulk equipment interference and the retention and examination of bulk personal datasets ("BPD").
4. SIS has set out in writing details of the safeguarding arrangements it has in place before the issuing authority can issue a warrant under the relevant powers in the Act. These documents are usually referred to as "Handling Arrangements". Where these Handling Arrangements have been relied on to date, they have been approved by the relevant Secretaries of State. The Investigatory Powers Commissioner has been provided a copy of these arrangements in parallel.

SIS Handling Arrangements

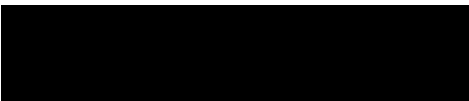
5. Details of the safeguarding arrangements which SIS currently has in place for to ensure its compliance with the provisions of the Act are set out in a document entitled

"INVESTIGATORY POWERS ACT 2016 – SIS HANDLING AND SAFEGUARDING ARRANGEMENTS", a copy of which is attached. This document contains a limited number of redactions which are necessary for the protection of national security, e.g. details of SIS processes which would give advantage to the UK's adversaries.

6. SIS's Handling Arrangements referred to above are supported and underpinned by other, more detailed, internal handling arrangements and policies. These policies include guidance to SIS staff which is tailored to specific work areas and the handling of any material which is subject to additional safeguards, such as journalistic material, material to which LPP might apply or other information which may be subject to additional confidentiality requirements. Individual SIS warrants provide the Secretary of State with details of the handling arrangements relevant to the decision they are taking. A copy of the application will be provided to IPCO. The individual SIS internal handling arrangements and policies contain highly classified information, the disclosure of which would be prejudicial to national security.
7. The Second Defendant is aware that SIS has internal policies underpinning the Handling Arrangements, but has not systematically been provided with the detail or totality of those policies. However, these policies are subject to independent oversight by IPCO, who have been fully briefed on SIS systems and policies relevant to their role. IPCO can conduct ad hoc additional inspections on any policy area, and can draw on independent technical expertise where they deem it necessary.
8. I am satisfied that SIS's Handling Arrangements fully comply with the requirements of the Act. As stated above, the Second Defendant has approved the SIS Handling Arrangements.

Statement of Truth

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


Dated: 4th February 2019



Foreign Secretary

**INVESTIGATORY POWERS ACT 2016 – SIS HANDLING AND SAFEGUARDING
ARRANGEMENTS**

Introduction

1. The Investigatory Powers Act 2016 requires the Secretary of State to ensure that SIS has in force certain safeguarding arrangements before issuing an IPA warrant. This document explains the safeguarding arrangements that SIS has in place. The Secretary of State is asked to agree that these arrangements are satisfactory. The Investigatory Powers Commissioner has been sent a copy of these arrangements in parallel.
2. If the Secretary of State is satisfied, SIS will not ordinarily explain the relevant safeguarding arrangements in an application for an IPA warrant, rather in each application SIS will remind both the Secretary of State and the Judicial Commissioner reviewing the approval of the Secretary of State that the safeguarding arrangements have been agreed, and that they will apply to the warrant in question. Each Judicial Commissioner reviewing SIS applications will be provided with a copy of this document together with the Secretary of State's confirmation.
3. SIS will keep these arrangements under review and will make any change to these arrangements known to the Secretary of State as soon as reasonably practicable.

Safeguards required in relation to equipment interference

4. Sections 129 and 130 provide for safeguards relating to the retention and disclosure of material obtained under a targeted equipment interference warrant which are very similar, but not entirely identical, to those in sections 53 and 54 in relation to material obtained by targeted interception.
5. Section 129 says in relation to every targeted equipment interference warrant issued, the Secretary of State, as issuing authority must ensure that arrangements are in force for securing that the requirements of subsections 129(2) and 129(5) are satisfied.
6. Subsection 129(2) requires that in relation to any material obtained under a warrant - the number of persons to whom that material is disclosed or otherwise kept available, the extent to which any material is disclosed or otherwise made

available, the extent to which material is copied and the number of copies that are made – is limited to the minimum necessary *for the authorised purposes*.

7. These arrangements must include arrangements for securing that every copy made of any of the material is stored, for so long as it is retained, in a secure manner.
8. For the purposes of Section 129 something is necessary *for the authorised purposes* if, and only if, -
 - a. It is necessary on any of the grounds upon which the Secretary of State may consider a targeted equipment interference warrant is necessary; in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security,
 - b. It is necessary for facilitating the carrying out of any functions under the IPA of the Secretary of State, the Scottish Ministers or C, as the person to whom SIS warrants will be addressed,
 - c. It is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to the IPA,
 - d. It is necessary for the purpose of legal proceedings, or,
 - e. It is necessary for the performance of any functions of any person under any enactment.
9. In this context a copy means any copy, extract or summary of the material which identifies the material as having been obtained under the targeted equipment interference warrant and any record of the identities of the persons who owned, used or were in possession of the equipment which was interfered with in order to obtain that material.
10. Subsection 129(5) requires the destruction of every copy made of the material obtained under a targeted equipment interference warrant, if not destroyed earlier, as soon as its retention is not necessary, or not likely to become necessary, on any of the grounds upon which the Secretary of State may consider an equipment interference warrant is necessary; the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security, and its retention is not necessary for any of the purposes in paragraph 16 b to e (above).
11. Section 130 in effect gives the Secretary of State discretion to decide whether, and if so to what extent, (a) the safeguards required by subsections 129(2) and 129(5), should apply to any material obtained under a warrant, or any copy of any such material, that is disclosed to an overseas authority. If the Secretary of

State decides that these safeguards should apply to any extent, to any such material or copy of such material, then Section 130 requires the Secretary of State to ensure that in relation to every targeted equipment interference warrant, arrangements are in force for ensuring that any material obtained under the warrant or any copy of any such material is only handed over to overseas authorities if these requirements are met.

12. In contrast to targeted interception there is no prohibition on the disclosure in proceedings of material obtained under a targeted equipment interference warrant (no "evidential bar"), and therefore no equivalent arrangements are required.

Arrangements in force to satisfy the requirement for safeguards in relation to the interception of communications and equipment interference

13. The following arrangements are implemented by SIS to satisfy the requirement for safeguards in relation to the interception of communications and equipment interference material as set out above. They apply in respect of intercepted and equipment interference material to the extent that such material identifies itself as the product of an interception or equipment interference warrant. These arrangements are supported by SIS's *** Policy, supplemented by detailed internal guidance on the handling and disclosure of intercept and equipment interference material, including specific arrangements for the handling of Legal Professionally Privileged (LPP) and confidential material.

14. For this purpose, "intercept material" includes, but is not limited to:

- a. original recordings of call/communication content;
- b. electronic/digital communications;
- c. secondary data obtained through interception;
- d. related systems data obtained through interception;
- e. any record referring to an interception which is the record of the identities of the persons to or by whom the intercept material was sent, or to whom the communications data relates;
- f. All copies, transcripts, extracts or summaries of the above.

15. For this purpose, "equipment interference material" includes, but is not limited to:

- a. any data obtained from electromagnetic equipment, including communications, equipment data and any other information;
- b. original recordings from surveillance conducted by means of equipment interference;
- c. all copies, transcripts, extracts or summaries of any of the above.

16. These arrangements in so far as they relate to the disclosure of intercept material and equipment interference material also apply to all disclosures of the following, irrespective of whether any communication content or equipment data is disclosed:

- a. the existence or contents of an interception or equipment interference warrant;
- b. details of the issue, renewal or modification of an interception or equipment interference warrant;
- c. any steps taken in pursuance of a warrant or a requirement to provide assistance in giving effect to a warrant.

Storage, access and copies:

17. All intercept material and equipment interference material in the possession of SIS will be stored securely in SIS premises which are subject to the highest standard of physical security. ***
18. Members of SIS should access intercept material and equipment interference material only where and to the extent that it is necessary and proportionate in the proper pursuit of the SIS's statutory functions. Intercept and equipment interference material will be copied only so far as is necessary and proportionate for the proper discharge of the statutory functions of SIS.
19. All members of SIS with access to intercept material and equipment interference material are subject to a high quality security vetting regime, including enhanced vetting for system administrators. In addition, all members of SIS with access to such information will have undertaken relevant training, including mandatory training where appropriate.
20. All SIS systems holding intercept material or equipment interference material must be designed and configured as far possible to facilitate the effective application of IPA and other legal requirements, in line with SIS's *** policy.
21. All intercept material and equipment interference material held on SIS systems will be held subject to appropriate *** controls and access to such material on SIS systems is subject to meeting the conditions of 'need to know' and users having appropriate security clearances. Access to intercept material and equipment interference material held within SIS systems is governed by access groups with access granted on the basis of necessity for a given role.
22. All user activity on SIS systems is subject to internal audit and accounting.

Retention and Destruction:

23. Intercept material and equipment interference material will be retained if that retention is, continues to be, or is likely to become, necessary for purposes set out in paragraphs x and x above.
24. All intercept material and equipment interference held by SIS is retained in accordance with SIS's *** policy and retention schedules. Such material is subject to regular review to ensure the case for retaining it remains necessary for

any of the purposes specified in paragraphs x and x above. Intercept material and equipment interference material must be deleted and scheduled for destruction as soon as it is assessed that there are no longer grounds for retaining it as necessary, or likely to become necessary, for any of the purposes specified in paragraphs x and x above.

25. Where it is possible, relevant SIS systems are configured to automatically delete intercept material and equipment material after the appropriate default retention period. Where interception or equipment interference errors are identified, relevant data is purged immediately from affected repositories.

Procedures for disclosure outside of SIS:

26. The following procedures apply for the purposes of authorising excepted disclosures under sections 58 and 133 of the IPA:
27. All disclosure by SIS of intercept material and equipment interference material is subject to Section 2(2)(a) of the Intelligence Services Act 1994 which requires that SIS disclose information to the minimum extent necessary for the proper discharge of its statutory functions and that no information is disclosed by it except so far as necessary for the proper discharge of its functions, in the interests of national security, for the prevention or detection of serious crime or for the purpose of any criminal proceedings.

Disclosure of *** material

28. *** material may be disclosed by SIS in so far as it is assessed to be necessary and proportionate to do so under section 2(2)(a) of the Intelligence Services Act 1994 and in accordance with SIS's *** policy.

Disclosure of *** material

29. This is material the format or content of which identifies it expressly or implicitly as having been obtained under an interception or equipment interference warrant.
30. If authorisation is obtained where required (see paragraphs *** below) *** intercept and equipment interference material may be disclosed if, and only if, such disclosure is **necessary**:
- a. for the proper discharge of SIS's statutory functions;
 - b. for the purpose of the prevention or detection of serious crime;
 - c. for the purpose of criminal proceedings;
 - d. for facilitating the carrying out of any functions under the IPA of the Secretary of State or Scottish Ministers;
 - e. for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to the IPA;

and is **proportionate** to the objective of the disclosure.

31. Intercept material may also be disclosed if, and only if, it is or is likely to become necessary:

- a. to ensure that a person conducting a criminal prosecution has the information they need to determine what is required of them by their duty to secure the fairness of the prosecution; or
- b. for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923

and is proportionate to the objective of the disclosure.

32. Equipment interference material may also be disclosed if, and only if, that disclosure is or is likely to become necessary:

- a. for the purpose of legal proceedings;
- b. for the performance of any functions of any person under any enactment;

and is proportionate to the objective of the disclosure.

Authorisation levels for disclosure of *** material

33. Appropriate team leaders may, on the advice of a *** (or equivalent) or above member of the SIS warrantry team, disclose intercept material or equipment interference material without specific authorisation:

34. Any officer of *** (or equivalent) or above may authorise disclosure of *** intercept material or EI material by them or another:

35. An officer of at least *** (or equivalent) may authorise disclosure of *** intercept material or equipment interference material by them or another officer:

36. All other disclosures of the fact of intercept or equipment interference or of intercept material or equipment interference material require the authority of a Director (or above) (see paragraphs x and x below).

Further dissemination

37. The quantity of *** intercept material or equipment interference material disclosed and the number of persons to whom the material is disclosed will be limited to the minimum necessary for the purpose for which disclosure is made.

38. SIS will ensure that *** intercept material and equipment interference material is disclosed on the following basis:

- a. that it should not be further disseminated without the prior authority of SIS; and
- b. that it should be returned to SIS or securely destroyed once it is no longer needed for a purpose for which such material can be lawfully retained, or otherwise at the request of SIS.

Disclosure to overseas authorities

Disclosure of *** intercept and equipment interference material to overseas authorities *** can be authorised as set out at paragraph ***

Safeguards relating to bulk personal datasets

39. Sections 204 and 205 require the Secretary of State to consider that, in relation to every class bulk personal dataset (BPD) warrant or specific BPD warrant, the arrangements made by the intelligence service for storing bulk personal datasets and for protecting them from unauthorised disclosure are satisfactory.
40. Section 221 requires the Secretary of State to ensure that, in relation to every class BPD warrant or specific BPD warrant, arrangements are in force for securing that any selection of data for examination is carried out only for the *specified purposes*, and that selection of data for examination is necessary and proportionate in all the circumstances. Subsection 221(2) says that selection of data for examination will be carried out only for the specified purposes, if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant.

Arrangements in force to satisfy the requirement for safeguards in relation to bulk personal datasets

41. The following arrangements are implemented by SIS to satisfy the requirement for safeguards in relation to the storage, selection for examination and disclosure of data retained under class and specific BPD warrants. These arrangements apply to all BPDs acquired by SIS including those in relation to which a Secretary of State's direction is made under section 225(3) IPA. These arrangements are supported by SIS's detailed internal BPD handling arrangements and associated internal policy and guidance documentation.

Storage and access

42. All BPDs in the possession of SIS will be stored securely in SIS premises which are subject to the highest standard of physical security.
43. All members of SIS with access to BPDs are subject to a high quality security vetting regime, including enhanced vetting for system administrators and other data specialist users with privileged access. Access to BPDs is permitted only where and to the extent necessary in the proper pursuit of the SIS's statutory functions. All BPDs held on SIS systems will be held subject to appropriate ***

controls and access to BPDs on SIS systems is subject to meeting the conditions of 'need to know' and users having appropriate security clearances.

44. SIS staff can only have access to BPDs if, in their role, it is necessary, proportionate and there is an appropriate business need to do so. Access to BPD on SIS systems will only be approved if the user has undertaken mandatory BPD training and has signed a copy of *** and the relevant *** Codes of Practice which outlines the appropriate use of each BPD system within SIS.
45. All SIS systems holding BPDs must be designed and configured as far possible to facilitate the effective application of IPA requirements, in particular to prevent any unauthorised access to BPDs, to any protected data with conditions imposed by the Secretary of State and LPP material within BPDs.
46. All user activity on SIS systems is subject to internal audit and accounting. SIS will maintain robust data security and protective security standards for BPDs. Further guidance is found in SIS's internal BPD handling arrangements which requires that the integrity and confidentiality of the information in the BPD is effectively protected, 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 it is detected and that appropriate disciplinary action is taken.

Selection for examination

All BPD warrants

47. Data contained in BPDs must only be selected for examination if:
 - a. selection is carried out for one or more of the operational purposes specified in the class or specific warrant under which the BPD is retained; and
 - b. selection for examination is necessary and proportionate in all the circumstances.
48. SIS has detailed internal BPD handling arrangements and mandatory training in place to help ensure that users examine BPD in accordance with required safeguards. In particular, users are required to demonstrate that their examination of BPD is necessary and proportionate, is justified in sufficient detail, and is carried out for an appropriate operational purpose. Before all examination of BPD, users are also required to ensure that they have appropriately considered all lesser intrusive methods (e.g. searching of corporate records or targeted data stores).

Specific BPD warrants

49. In the case of BPDs retained under specific warrants, protected data must only be selected for examination on the basis of criteria referable to a person known to be in the British Islands at the time of selection in accordance with any conditions specified in that warrant.

50. Further guidance on selection for examination of protected data is found in SIS's internal handling arrangements. In particular, SIS systems holding BPD protected data system must not allow the user to see Protected Data unless conditions imposed by the Secretary of State on the specific BPD warrant for the BPD have been met.

Disclosure outside SIS

51. Disclosure of BPDs or information in BPDs must be made in accordance with SIS's internal handling arrangements. 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 ***. Disclosure is authorised under the information gateway provisions of the ISA 1994.
