APPENDIX 2 TO JUDGEMENT OF 23 JULY 2018

Handling Arrangements and other guidance in relation to sharing BPD/BCD outside the SIA

Double-underlining within extracts indicates gisting.

Statutory safeguards

1) The regime in respect of Bulk Personal Datasets ("BPD") and Bulk Communications Datasets ("BCD") which is relevant to sharing by the Intelligence Services with foreign liaison/LEAs/industry partners principally derives from the following statutes:

   a) the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA");

   b) the Counter-Terrorism Act 2008 ("the CTA");

   c) the Human Rights Act 1998 ("the HRA");

   d) the Data Protection Act 1998 ("the DPA"); and

   e) the Official Secrets Act 1989 ("the OSA").

2) There are also important **oversight mechanisms** in the regime provided by the Interception of Communications Commissioner and the Intelligence Services Commissioner (both of whom were replaced, on 1 September 2017, by the Investigatory Powers Commissioner) and by the Intelligence and Security Committee and the Tribunal. These mechanisms have already been considered and approved by the Tribunal in its October 2016 judgment. However, the Commissioners' role in relation to disclosure/sharing of BPD/BCD is addressed below.

The SSA and ISA

Security Service functions

3) By s.1(2) to (4) of the Security Service Act 1989 ("SSA"), the functions of the Security Service are the following:

"the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."

"to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

"to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime."

4) The Security Service's operations are under the control of a Director-General who is appointed by the Secretary of State (s.2(1)). By s.2(2)(a) it is the Director-General's duty to ensure:

"…that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;…"

SIS functions

5) By s.1(1) of the ISA, the functions of SIS are:

"(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

(b) to perform other tasks relating to the actions or intentions of such persons."

6) By s.1(2) those functions are *"exercisable only-*

"(a) in the interests of national security, with particular reference to the defence and foreign polices of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime."

7) SIS's operations are under the control of a Chief, who is appointed by the Secretary of State (s.2(1)). The Chief of SIS has a duty under s.2(2)(a) of the ISA to ensure:

"(a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary-

(i) for that purpose;

(ii) in the interests of national security;

(iii) for the purpose of the prevention or detection of serious crime; or

(iv) for the purpose of any criminal proceedings;…"

GCHQ functions

8) By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."

9) By s. 3(2) of the ISA, these functions are only exercisable:

"*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime."

10) GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ...*"

11) The functions of each of the Intelligence Services, and the purposes for which those functions may properly be exercised, are thus prescribed by statute. In addition, the duty-conferring provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, otherwise known as *"the information gateway provisions"*, place specific statutory limits on the information that each of the Intelligence Services can obtain and disclose. These statutory limits apply to the obtaining and disclosing of information from or to other persons both in the United Kingdom and abroad.

Counter-Terrorism Act 2008

12) By s.19(1) of the Counter-Terrorism Act 2008 ("CTA") *"A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions."*

13) By s. 19(2) of the CTA:

> "*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

14) By s.19(3) to (5) of the CTA, information obtained by the Intelligence Services for the purposes of any of their functions may:

a) In the case of the Security Service *"be disclosed by it – (a) for the purpose of the proper*

discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings." (s.19(3))

b) In the case of SIS *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings."* (s.19(4))

c) In the case of GCHQ "*be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*." (s.19(5))

15) By s.19(6) any disclosure under s.19 "*does not breach* –

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed)."

16) Furthermore:

a) s.19 does not affect the duties imposed by the information gateway provisions (s.19(7) and s.20(1) of the CTA).

b) by s.20(2) of the CTA, nothing in s.19 *"authorises a disclosure that-*

(a) contravenes the Data Protection Act 1998 (c.29), or

(b) is prohibited by Part 1 of the Regulations of Investigatory Powers Act 2000 (c.23)."

17) Thus, specific statutory limits are imposed on the information that the Intelligence Services can obtain, and on the information that it can disclose under the CTA.

The HRA

18) Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."

19) By s. 6(1):

"*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

20) Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Respondents must (among other things) act proportionately and in accordance with law. In terms of BPD/BCD-related activity, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

21) S. 7(1) of the HRA provides in relevant part:

"*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—*

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."

The DPA

22) Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data that it holds. "Personal data" is defined in s.1(1) of the DPA as follows:

"data which relate to a living individual who can be identified-

i. from those data; or

ii. from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

23) Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

24) Consequently as a data controller, the Respondents are in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5. Personal data processed*[1] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[2]

25) Accordingly, when the Respondents obtain any information which amounts to personal data, they are obliged:

a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

[1] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.
[2] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

26) A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of any of the Respondents that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

27) Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

BULK PERSONAL DATASETS

Cross-SIA Policy

28) The Joint SIA BPD Policy, which came into force in February 2015 sets out agreed policy for each of GCHQ, the Security Service and SIS for sharing BPD:

> "**D. Sharing**
>
> 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 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..."

29) The OPEN BPD Handling Arrangements which came into force in November 2015 address disclosure of BPD at §§5.2, 6.1-6.7 and 8.1:

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

"6.0 Procedures and Safeguards for Disclosure of Bulk Personal Datasets outside the relevant Intelligence Service

6.1 Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:

- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective;
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

When will disclosure be necessary?

6.2 In order to meet the '**necessity'** requirement in relation to disclosure, staff must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.

The disclosure must also be "proportionate"

6.3 The disclosure of the bulk personal dataset must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal dataset.

6.4 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.

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

6.6 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.

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

30) In addition:

"8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Services 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 discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective."

Action On Process

31) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

Commissioner oversight

32) By the Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015, the Prime Minister, pursuant to his power under s.59(a) of RIPA, directed the Intelligence Services Commissioner to *"continue to keep under review the acquisition, use, retention and* ***disclosure*** *by the* [SIAs] *of bulk personal datasets, as well as the adequacy of safeguards against misuse."* and to *"assure himself that the acquisition, use, retention* ***and disclosure*** *of bulk personal datasets does not occur except in accordance with"* the relevant sections of the SSA 1989 and ISA 1994 and to *"seek to assure himself of the adequacy of the [SIAs'] handling arrangements and their compliance therewith."* (emphasis added)

33) Before 1 September 2017, the Intelligence Services Commissioner had oversight and access to all SIA material in relation to BPD/BCD compliance, including that relating to sharing. For the avoidance of doubt, that would extend to any activity of the SIA, were it to take place, relating to BPDs, including sharing with partners or giving partners remote access. In answer to a request by the Tribunal dated 13 April 2017 about what he regarded as within his remit the Intelligence Services Commissioner confirmed, by a letter to the Tribunal dated 27 April 2017 written jointly with the Interception of Communications Commissioner, that both "use" and "disclosure" are *"taken to include sharing with other agencies or organisations, including foreign agencies."* Since 1 September 2017 the Intelligence Services Commissioner's functions have been performed by the Investigatory Powers Commissioner.

Breaches of safeguards

34) In the event that any of the SIAs' policies and safeguards in respect of sharing BPD were breached, the relevant Agency would report any such breach to the Intelligence Services Commissioner (or now the Investigatory Powers Commissioner); investigate the breach; consider whether it remained lawful or appropriate to continue to share; if and to the extent that any Agency staff had committed the breach in question, consideration would be given to disciplinary proceedings.

GCHQ

35) Section 9 of the GCHQ BPD Handling Arrangements which came into force in November 2015 addresses disclosure of BPD at section 9:

> "**9. Disclosure**
> 9.1 Where the results of bulk personal data analysis are disclosed to partner or customer organisations, this must be done via standard reporting mechanisms, which ensure release of GCHQ intelligence in a secure, accountable, legally compliant manner.
> 9.2 If disclosure of a bulk personal dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed:
> ...
>
> [REDACTED]
> 9.4 Other organisations:
> 9.4.1 For any other organisation, whether another UK partner or a *foreign partner*, the dataset's Requester or Endorser will submit a request for authorisation to disclose, by means of the dataset's BPD form. Again, such requests will be considered by *relevant GCHQ senior officials*.
> 9.5 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of:
> – its necessity and proportionality, and
> – the intelligence or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.
> 9.6 The Authoriser will consider:
> – the content of the dataset: the nature of the personal information it contains, its intrusiveness and sensitivity;
> – the nature and extent of the corporate risk the disclosure would entail;
> – the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
> – whether any caveats or restrictions should be applied; and
> – the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary."

36) The form referred to at §9.4.1 of the GCHQ BPD Handling Arrangements is GCHQ's Bulk Personal Data Acquisition Retention (BPDAR) form, which, *inter alia*:

a) Requires the necessity and proportionality case for sharing BPD to be set out *"if it is proposed to share some or all of [the] dataset with an external organisation other than that which provided the data to GCHQ in the first place."* ; and

b) Requires identification of whether the BPD contains any sensitive personal data, and if so what kind .

GCHQ Policy on sharing BPD with foreign liaison/LEAs

37) GCHQ operates on the basis that operational data of any sort may only be shared if it is necessary for one of GCHQ's statutory functions, and, as far as GCHQ's intelligence gathering function is concerned, in line with one of the three purposes for which that function can be exercised. This is set out in GCHQ's Compliance Guide. All sharing is subject to compliance with all relevant legal safeguards, and there is a requirement that recipients must accord the material a level of protection equivalent to GCHQ's own safeguards. The assessment of whether a partner's safeguards meet this standard is a matter for the Mission Policy team, in partnership with departmental legal advisors and other specialist teams as appropriate. As a matter of policy GCHQ applies the safeguards required by RIPA to all operational data even if was not obtained under RIPA powers, so this is the standard that must be met. Sharing is also subject to policy approval by an appropriately senior member of the Mission Policy team, unless an explicit delegation of approval authority has been made. Policy approval may be subject to appropriate filtering or sanitisation of the data being applied to protect sensitive material or equities.

38) The Compliance Guide makes clear that, in line with the RIPA Interception of Communications Code of Practice, particular consideration should be given in cases where confidential information (which includes, inter alia, material that is legally privileged, and confidential journalistic information) is involved. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of such material is necessary and proportionate. This covers any sharing of such data with partners. Any sharing of BPD in whole or in part is subject to formal approval by Deputy Director Mission Policy who will take into account the potential for such data to contain confidential information and ensure that this is removed from the data to the extent possible (e.g. by the removal of particular fields from datasets) and will require the application of additional or more stringent safeguards where appropriate.

39) Were GCHQ to share BPD with foreign liaison or LEAs, then it would:

a) Follow the principles and approach set out in their respective Handling Arrangements and policy/guidance.

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

c) Take into account the nature/remit of the body to which they were considering disclosing the BPD.

d) Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understanding that the other agencies may have used/followed.

e) Depending on the individual circumstance, seek assurances that the BPD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purposes of RIPA (in the interests of National Security, for the purpose of preventing or detecting Serious Crime, or for the purpose of safeguarding the economic well-being of the UK.

40) In addition, were GCHQ to give liaison partners and/or law enforcement agencies remote access to run queries to BPD, it would apply safeguards which would put partner analysts on the same basis as GCHQ analysts. In particular, GCHQ would:

a) Require analysts to have completed all relevant training (including legalities training), be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances;

b) Require all queries to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ;

c) Require analysts to comply with GCHQ's Compliance Guide and other BPD policies and safeguards concerning access, retention and use (as set out in the Cross-SIA and GCHQ BPD Handling Arrangements);

d) Comply with the safeguards regarding the treatment of LPP and journalistic material addressed in the required training and the Compliance Guide.

<u>GCHQ policy on sharing BPD with industry partners</u>

41) GCHQ may share operational data with industry partners for the purpose of developing and testing new systems. Actual operational data would only be shared for such purposes if it were not possible to use standardised corpuses of non-operational data. Any sharing would be of the minimum volume of data necessary to develop or test the system. In all cases the data would be the least intrusive data that can serve the purpose. For this reason any data known or believed to contain confidential information would not be used; similar data that does not contain such material would be used instead. Wherever possible data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that the data must be

held on secure and accredited corporate premises in the UK. All sharing of data with industry is recorded on a Raw Data Release Request form which must be completed by a member of GCHQ who is sponsoring the activities of the industry partner. This form (which is used for certain other forms of data sharing which do not involve BPD) requires the sponsor to describe the purpose of the sharing and the details of the data they wish to release. If the data is to leave GCHQ premises they must specify where it is to go, and how it will be transferred. The form requires the sponsor to detail the name, organisation and job title of the individual who will take responsibility for the data on receipt, how many people at the recipient organisation will have access, for how long the data will be retained and what will be done with it once the project is completed. These requests are assessed within the Mission Policy team and may be escalated up to the Deputy Director Mission Policy where appropriate. Mission Policy will assess each proposal to ensure that the sharing is both necessary and proportionate, and may require modification of the request if there are concerns about proportionality.

Security Service

42) The MI5 BPD guidance of March 2015 addressed sharing/disclosure of BPD as follows:

> "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) as 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 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*.

In the event that a formal request is made to MI5 for BPD to be shared, the same legal disclosure tests would need to be applied as when sharing with BPD partners. The requestor would also require a legal gateway to acquire the data, which the Security Service would need to be satisfied met the test of necessity and proportionality. All enquiries should be directed to *the senior MI5 official*."

43) The Security Service BPD Handling Arrangements which came into force in November 2015 address disclosure outside the SIA in section 6:

"**6.0 Disclosure**

6.1 The disclosure of BPD is carefully managed to ensure that it 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*."

"6.2.1...Information in BPD held by MI5 can only be disclosed to persons outside the Service if the following conditions are met:

- that the objective of the disclosure falls within MI5's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is necessary to disclose the information in question in order to achieve that objective;
- that the disclosure is proportionate to the objective;
- that only as much of the information will be disclosed as is necessary to achieve that objective.

6.2.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the BPD is 'really needed' for the purpose of discharging a statutory function of MI5. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal data.

6.2.3 The disclosure of the BPD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of MI5's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved.

6.2.4 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BPD, a subset of the dataset, or an individual piece of data from the dataset.

6.2.5 Disclosure of **the whole (or a subset) of a bulk personal dataset** is subject to prior internal authorisation procedures in addition to the requirements in 6.2.1-6.2.3 above. Where these requirements are met, the BPD is formally requested by the requesting Agency from MI5 through an agreed disclosure procedure using *the relevant form*. The relevant data sponsor is then responsible for submitting *the relevant form* that will seek authorisation within MI5.

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 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."

44) The "relevant form" referred to at §§6.2.5, 6.2.6 and 6.3.2 of the Security Service BPD Handling Arrangements is the "Form for Sharing". It contains, *inter alia*, provision for:

a) Considering whether the BPD contains sensitive personal data, including but not restricted to journalistic and legally privileged material

b) Access restrictions: the *"arrangements agreed to ensure material is handled securely and what access control will be applied"* must be stated

c) Agreed caveats in relation to the handling of the material must also be set out

d) The "Business Justification & Privacy Assessment" requires the statutory purpose and a necessity and proportionality assessment to be set out, and approved by a senior MI5 official.

e) The technical feasibility of disclosure must be approved by the relevant technical team

f) Legal approval for disclosure must also be given by a legal adviser.

g) Final approval must also be given by DSIRO or designated person

Security Service Policy on sharing BPD with foreign liaison/LEAs/industry partners

45) Were the Security Service to share BPD with foreign liaison or LEAs, then it would only share if satisfied that:

a) Such sharing was for one of the Security Service's statutory purposes, or one of the limited additional purposes set out in s.2(2)(a) of the Security Service Act 1989.

b) It is necessary to disclose the information in question in order to achieve that objective;

c) That the disclosure would be proportionate to the objective;

d) That only as much of the information will be disclosed as is necessary to achieve that objective.

e) As set out at §6.3.2 of the Security Service BPD Handling Arrangements, the Security Service would also (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 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.

46) In the event that MI5 were considering sharing or were to share bulk data, then the approach that it would take, and the principles that it would apply, would be as described below.

47) The principles and approach that it would apply can be summarised as follows:

a) An information gathering exercise would be conducted in relation to the proposed recipient.

b) If that was satisfactory, then a sharing agreement would be prepared, if deemed necessary, to reflect the matters that MI5 considered (having regard to the information gathering exercise) needed to be covered.

c) Individual consideration of each bulk dataset to be shared would be carried out. If agreed, then any sharing of bulk datasets would be accompanied by specific handling instructions, setting out any particular requirements considered appropriate.

d) Ongoing review of the sharing relationship would be conducted.

<u>Stage 1 – information gathering</u>

48) In advance of initial sharing, and to inform the decision-making process to do so, an information gathering exercise would be undertaken to better understand the legal framework, policy and practice of the recipient. Specifically this exercise would gather information in the following areas which would inform decision making and any written agreements that were deemed appropriate:

a) Law and Policy – identifying the legal and policy regime that would apply in relation to bulk datasets in the recipient.

b) Acquisition of Bulk Data – identifying (if any) the process which would be applied before the recipient acquires bulk datasets and whether there is any legal and/or policy obligation to consider the necessity and proportionality of acquiring a particular dataset.

c) Authorisation – identifying the process and requirements (if any) that would be applied to authorise the retention and examination of bulk datasets.

d) Ingestion and Access – identifying how shared data would be stored, any categories of data the recipient considers sensitive (for example legal professional privilege) either by law or policy and any policy governing access to the raw dataset or intelligence derived from it.

e) Exploitation and Analysis – make reasonable enquiries regarding the use that would be made of the bulk data and the capabilities of the systems on which it would be used.

f) Disclosure – identifying any ACTION ON procedures or safeguards and the considerations taken into account when deciding to share bulk data with others.

g) Retention and Review – identifying the process and parameters by which the necessity and proportionality case for continuing to retain and exploit bulk data would be reviewed.

h) Oversight – identifying what internal and external oversight arrangements would be in place to audit the acquisition, retention and exploitation of bulk data.

49) In addition, in the event of any sharing of bulk data outside the SIA, MI5 would ensure that sharing of that data is in accordance with any wider HMG policies which MI5 is required to adhere to (for example HMG Consolidated Guidance).

Stage 2 – Sharing agreement

50) Subject to MI5 being satisfied following its information gathering exercise, a written agreement would, if considered necessary, be agreed between the recipient and MI5 in advance of any bulk data sharing. Insofar as considered appropriate, MI5 would require the recipient to apply

safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements. A written agreement may detail (taking into account the results of the information gathering exercise) requirements for the following aspects of sharing:

a) How shared data will be stored, accessed and used.
b) An agreed security classification for the shared data.
c) Suitable technical and organisational measures to protect data from accidental or unauthorised disclosure or misuse.
d) A requirement that permission be sought from the disclosing partner prior to any onward disclosure from the recipient of all or part of a bulk dataset or any targeted data derived from it.
e) A requirement that permission be sought from the disclosing partner prior to any executive action being undertaken by the recipient on the basis of any shared data or targeted data derived from it.
f) A requirement that disclosure of and access to any shared data be limited to appropriately cleared personnel within the recipient who have a business justification for access to the data.
g) All staff within the recipient with access to the shared data will be made aware of the provision governing the retention and examination of the shared data made within the written agreement.
h) A requirement for the destruction of the shared data as soon as its retention is no longer deemed to be necessary or proportionate.
i) A requirement to inform the disclosing partner of any threat to life reporting obtained from examination of the shared data.
j) An assessment that the sharing of data complies with the disclosing partner's legal obligations and that the receipt of the data by the receiving partner complies with their legal obligations.

<u>Stage 3 – Individual consideration of each bulk dataset to be shared and the terms of handling instructions to accompany each bulk dataset shared</u>

51) In every instance where sharing of bulk data were proposed then there would need to be particular consideration of that proposed sharing, having regard to the terms of any sharing agreement in place. In each case where a bulk dataset were shared with a partner, specific handling instructions would accompany it. In addition, insofar as considered appropriate, MI5 would require the recipient to apply specific safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements appropriate to the nature of the data being shared.

<u>Stage 4 – Review</u>

52) Were sharing of bulk data to occur, MI5 would maintain the following ongoing obligations:

a) Undertake reviews to ensure the necessity and proportionality case for sharing continued to exist.

b) Undertake reviews of the adequacy of the arrangements governing the sharing with each recipient, including Action On, as and when necessary.

c) End current sharing with a recipient if judged necessary as a result of the above.

d) Inform the recipient of any changes to MI5's legal obligations impacting on bulk data sharing and update, as necessary, any written agreements and/or handling instructions.

SIS

53) SIS's Bulk Data Acquisition, Exploitation and Retention policy provided from 2009 onwards that:

> "17. Bulk data can be shared with other third parties (eg a liaison partner) with the Data Owner's permission and subject to certain assurances. *Were there to be such sharing, the assurances would require a liaison to handle the data securely, not to share it further without permission, and to share, as far as is practicable, results that have an impact on UK on UK National Security*."

54) SIS BPD Handling Arrangements, which came into force in November 2015 , include specific guidance to staff on the sharing of BPD with foreign partners, including:

> "7.1 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 resists with the *senior SIS official*."

55) The guidance also states that:

> "7.3.1 *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.

7.3.2 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*."

SIS Policy on sharing BPD with foreign liaison and LEAs

[See SIS's statement of 3 March 2017, §§10-24]

56) Should SIS decide that there were 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).

57) Further, specifically in relation to foreign liaison and LEAs, SIS would consider any proposal to share on a case by case basis, taking into account a number of factors:

a) The nature of the partner with whom they would be sharing. This includes considering the history SIS has of sharing intelligence with that partner; their data capability and practices; and their history of compliance, either where SIS has previously shared data or where SIS has 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 understand that the recipient partner wishes to obtain BPD.

Due diligence

58) The due diligence exercise would seek assurances from the proposed recipient on the relevant aspects of that partner's governance. The aim would be to establish that they have in place equivalent standards as would apply to the Agency's own staff and procedures. In practice, the specific nature of this due diligence exercise may well be tailored on a case by case basis and be subject to, for example, the particular context of the proposed arrangements or the nature of the existing relationship with that partner. The sorts of questions that SIS would seek satisfactory answers to in order to provide satisfactory 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 partner organisation subject to provisions in law (international or domestic) that would govern their use of bulk data? Are they governed by any statutory requirements that would tie their use of bulk data 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 partner organisation take into account before acquiring bulk data? 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 partner 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 bulk data? Are there categories that would be considered sensitive or privileged either by law or policy? Would ingestion of data of this type 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 partner 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 bulk data? 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 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 meets certain criteria? How would a user know that a particular piece of data requires Action On before they can 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?

59) 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 the recipient partner would handle BPD (covering all the matters set out at paragraph 58 above); as well as the domestic legal and compliance regime to which they are required to adhere.

60) Any such due diligence exercise would necessarily be bespoke and tailored to the partner in question and the particular circumstances of the proposed sharing arrangement. The questions set out in paragraph 58 are illustrative and neither exhaustive nor a pro forma. 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 partner's governance arrangements. It is likely that SIS would seek to validate assurances given by means of 'in person' discussions with responsible officers of the partner organisation and by reference to internal policy documents, forms, codes of practice and training materials.

61) If a due diligence exercise did not result in the obtaining of satisfactory assurances, or if the veracity of assurances obtained was in doubt, the Agency would not share bulk data. In any formalising agreement or memorandum of understanding, the Agency would set out the circumstances under which the arrangement could be halted if there was concern or evidence that arrangements were not satisfactory.

Agreement to share

62) 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.

Sharing of individual BPDs

63) 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.

64) SIS would ensure that dataset-specific handling instructions would accompany each BPD shared.

Monitoring compliance with assurances

65) 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 (see §31 above).

66) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

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

68) 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.

SIS Policy on sharing BPD with industry partners

69) Although SIS can neither confirm nor deny whether it has agreed to share or in fact shares BPD with industry partners, were it to do so, it would:

a) Follow the principles and approach set out in SIS's Handling Arrangements and policy/guidance;

b) Take into account the nature of the BPD that was due to be disclosed;

c) Take into account the nature of the body to which it was considering disclosing the BPD.

BULK COMMUNICATIONS DATASETS

Cross-SIA Policy

70) The OPEN BCD Handling Arrangements which came into force in November 2015 address disclosure of BCD (at §§4.4.1 to 4.4.6):

> "**4.4 Disclosure**
> 4.4.1 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of

an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official[3] or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:
- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective;
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

When will disclosure be necessary?

4.4.3 In order to meet the '**necessity'** requirement in relation to disclosure, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that disclosure of the BCD is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.

The disclosure must also be "proportionate"

4.4.4 The disclosure of the BCD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that the level of interference with the right to privacy of individuals whose communications data is being disclosed, both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of 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."

Action On Process

[3] Equivalent to a member of the Senior Civil Service.

71) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

Commissioner oversight

72) Before 1 September 2017, the Interception of Communications Commissioner had oversight and access to all SIA material in relation to BCD compliance, including that relating to sharing. For the avoidance of doubt, that would extend to any activity of the SIA, were it to take place, relating to BCDs, including sharing with partners or giving partners remote access. See:

a) MI5 BCD Handling Arrangements of November 2015, §4.6.4(b): *"The Interception of Communications Commissioner has oversight of...(b) MI5's arrangements in respect of acquisition, storage, access...and subsequent use,* ***disclosure****, retention and destruction"* (emphasis added); and

b) GCHQ BCD Handling Arrangements of November 2015, §4.6.9: *"The Interception of Communications Commissioner is responsible for overseeing* [inter alia] ***disclosure****...of the data"*.

c) In answer to a request by the Tribunal dated 13 April 2017 about what he regards as within his remit the Interception of Communications Commissioner has confirmed, by a letter to the Tribunal dated 27 April 2017 written jointly with the Intelligence Services Commissioner, that both "use" and "disclosure" are *"taken to include sharing with other agencies or organisations, including foreign agencies."*

Since 1 September 2017 the Interception of Communications Commissioner's functions have been performed by the Investigatory Powers Commissioner.

Breaches of safeguards

73) In the event that any of the SIAs' policies and safeguards in respect of sharing BCD were breached, the relevant Agency would report any such breach to the Interception of Communications Commissioner (or now the Investigatory Powers Commissioner); investigate the breach; consider whether it remained lawful or appropriate to continue to share; if and to the

extent that any Agency staff had committed the breach in question, consideration would be given to disciplinary proceedings.

GCHQ

74) Section 4.4 of the GCHQ BCD Handling Arrangements which came into force in November 2015 addresses disclosure of BCD:

> "**4.4 Authorisation of Disclosure**
> 4.4.1 Where the results of analysing section 94 data are disclosed to partner or customer organisations, this must be done via standard intelligence reporting mechanisms, which ensure that GCHQ intelligence is released in a secure, accountable and legally compliant manner.
> 4.4.2 If disclosure of a complete section 94 dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed.
> ...
> 4.4.6 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of
> – its necessity and proportionality, and
> – the intelligence benefit or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.
>
> 4.4.7 The Authoriser will consider:
> – the content of the dataset: the nature of any personal information it contains, its intrusiveness and sensitivity;
> – the nature and extent of the corporate risk the disclosure would entail;
> – the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
> – whether any caveats or restrictions should be applied; and
> – the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary."

GCHQ Policy on sharing BCD with foreign liaison/LEAs

75) GCHQ operates on the basis that operational data of any sort may only be shared if it is necessary for one of GCHQ's statutory functions, and, as far as GCHQ's intelligence gathering function is concerned, in line with one of the three purposes for which that function can be exercised. This is set out in GCHQ's Compliance Guide. All sharing is subject to compliance with all relevant legal safeguards, and there is a requirement that recipients must accord the material a level of protection equivalent to GCHQ's own safeguards. The assessment of whether a partner's

safeguards meet this standard is a matter for the Mission Policy team, in partnership with departmental legal advisors and other specialist teams as appropriate. As a matter of policy GCHQ applies the safeguards required by RIPA to all operational data even if was not obtained under RIPA powers, so this is the standard that must be met. Sharing is also subject to policy approval by an appropriately senior member of the Mission Policy team, unless an explicit delegation of approval authority has been made. Policy approval may be subject to appropriate filtering or sanitisation of the data being applied to protect sensitive material or equities.

76) The Compliance Guide makes clear that, in line with the RIPA Interception of Communications Code of Practice, particular consideration should be given in cases where confidential information (which includes, inter alia, material that is legally privileged, and confidential journalistic information) is involved. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of such material is necessary and proportionate. This covers any sharing of such data with partners. Any sharing of BCD in whole or in part is subject to formal approval by Deputy Director Mission Policy who will take into account the potential for such data to contain confidential information and ensure that this is removed from the data to the extent possible (e.g. by the removal of particular fields from datasets) and will require the application of additional or more stringent safeguards where appropriate.

77) Were GCHQ to share BCD with foreign liaison or LEAs, then it would:

a) Follow the principles and approach set out in their respective Handling Arrangements and policy/guidance.

b) Take into account the nature of the BCD that was due to be disclosed.

c) Take into account the nature/remit of the body to which they were considering disclosing the BCD.

d) Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understanding that the other agencies may have used/followed.

e) Depending on the individual circumstance, seek assurances that the BCD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purposes of RIPA (in the interests of National Security, for the purpose of preventing or detecting Serious Crime, or for the purpose of safeguarding the economic well-being of the UK.

78) In addition, were GCHQ to give liaison partners and/or law enforcement agencies remote access to run queries to BCD, it would apply safeguards which would put partner analysts on the same basis as GCHQ analysts. In particular, GCHQ would:

a) Require analysts to have completed all relevant training (including legalities training), be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances;

b) Require all queries to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ;

c) Require analysts to comply with GCHQ's Compliance Guide and other BCD policies and safeguards concerning access, retention and use (as set out in the Cross-SIA and GCHQ BCD Handling Arrangements);

d) Comply with the safeguards regarding the treatment of LPP and journalistic material addressed in the required training and the Compliance Guide.

GCHQ policy on sharing BCD with industry partners

79) GCHQ may share operational data with industry partners for the purpose of developing and testing new systems. Actual operational data would only be shared for such purposes if it were not possible to use standardised corpuses of non-operational data. Any sharing would be of the minimum volume of data necessary to develop or test the system. In all cases the data would be the least intrusive data that can serve the purpose. For this reason any data known or believed to contain confidential information would not be used; similar data that does not contain such material would be used instead. Wherever possible data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that the data must be held on secure and accredited corporate premises in the UK. All sharing of data with industry is recorded on a Raw Data Release Request form which must be completed by a member of GCHQ who is sponsoring the activities of the industry partner. This form (which is used for certain other forms of data sharing which do not involve BCD) requires the sponsor to describe the purpose of the sharing and the details of the data they wish to release. If the data is to leave GCHQ premises they must specify where it is to go, and how it will be transferred. The form requires the sponsor to detail the name, organisation and job title of the individual who will take responsibility for the data on receipt, how many people at the recipient organisation will have access, for how long the

data will be retained and what will be done with it once the project is completed. These requests are assessed within the Mission Policy team and may be escalated up to the Deputy Director Mission Policy where appropriate. Mission Policy will assess each proposal to ensure that the sharing is both necessary and proportionate, and may require modification of the request if there are concerns about proportionality.

Security Service

80) Paragraphs 4.4.1 to 4.4.8 of the Security Service BCD Handling Arrangements which came into force in November 2015 address disclosure of BCD:

"**4.4 Authorisation of Disclosure**

4.4.1 The disclosure of BCD is carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire BCD, or a subset, outside MI5 may only be authorised by the Home Secretary or a Senior Official[4] in the Home Office.

4.4.2 Disclosure of individual items of communications data to persons outside MI5 can only be made if the following conditions are met:
– The objective of the disclosure falls within MI5's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
– It is necessary to disclose the information in question in order to achieve that objective;
– The disclosure is proportionate to the objective;
– Only as much of the information will be disclosed as is necessary to achieve that objective.

4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the communications data is 'really needed' for the purpose of discharging a statutory function of that Agency. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion. For example, in cases where disclosure of BCD is contemplated, this could mean disclosure of individual pieces of data or of a subset of data rather than of whole BCD.

4.4.4 The disclosure of the communications data must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of MI5's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved.

[4] Equivalent to a member of the Senior Civil Service.

4.4.5 Before disclosing any communications 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.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BCD, a subset of the dataset, or an individual piece of data derived from the bulk communications dataset or from targeted communications data.

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."

Security Service Policy on sharing BCD with foreign liaison/LEAs/industry partners

81) Were the Security Service to share BCD with foreign liaison, LEAs or industry partners, then it would only share if satisfied that:

a) Such sharing was for one of the Security Service's statutory purposes, or one of the limited additional purposes set out in s.2(2)(a) of the Security Service Act 1989.

b) It is necessary to disclose the information in question in order to achieve that objective;

c) That the disclosure would be proportionate to the objective;

d) That only as much of the information will be disclosed as is necessary to achieve that objective.

e) As set out at §4.4.5 of the Security Service BCD Handling Arrangements, the Security Service would also (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 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.

82) In the event that MI5 were considering sharing or were to share bulk data, then the approach that it would take, and the principles that it would apply, would be as described below.

83) The principles and approach that it would apply can be summarised as follows:

a) An information gathering exercise would be conducted in relation to the proposed recipient.

b) If that was satisfactory, then a sharing agreement would be prepared, if deemed necessary, to reflect the matters that MI5 considered (having regard to the information gathering exercise) needed to be covered.

c) Individual consideration of each bulk dataset to be shared would be carried out. If agreed, then any sharing of bulk datasets would be accompanied by specific handling instructions, setting out any particular requirements considered appropriate.

d) Ongoing review of the sharing relationship would be conducted.

<u>Stage 1 – information gathering</u>

84) In advance of initial sharing, and to inform the decision-making process to do so, an information gathering exercise would be undertaken to better understand the legal framework, policy and practice of the recipient. Specifically this exercise would gather information in the following areas which would inform decision making and any written agreements that were deemed appropriate:

a) <u>Law and Policy</u> – identifying the legal and policy regime that would apply in relation to bulk datasets in the recipient.

b) Acquisition of Bulk Data – identifying (if any) the process which would be applied before the recipient acquires bulk datasets and whether there is any legal and/or policy obligation to consider the necessity and proportionality of acquiring a particular dataset.

c) Authorisation – identifying the process and requirements (if any) that would be applied to authorise the retention and examination of bulk datasets.

d) Ingestion and Access – identifying how shared data would be stored, any categories of data the recipient considers sensitive (for example legal professional privilege) either by law or policy and any policy governing access to the raw dataset or intelligence derived from it.

e) Exploitation and Analysis – make reasonable enquiries regarding the use that would be made of the bulk data and the capabilities of the systems on which it would be used.

f) Disclosure – identifying any ACTION ON procedures or safeguards and the considerations taken into account when deciding to share bulk data with others.

g) Retention and Review – identifying the process and parameters by which the necessity and proportionality case for continuing to retain and exploit bulk data would be reviewed.

h) Oversight – identifying what internal and external oversight arrangements would be in place to audit the acquisition, retention and exploitation of bulk data.

85) In addition, in the event of any sharing of bulk data outside the SIA, MI5 would ensure that sharing of that data is in accordance with any wider HMG policies which MI5 is required to adhere to (for example HMG Consolidated Guidance).

Stage 2 – Sharing agreement

86) Subject to MI5 being satisfied following its information gathering exercise, a written agreement would, if considered necessary, be agreed between the recipient and MI5 in advance of any bulk data sharing. Insofar as considered appropriate, MI5 would require the recipient to apply safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements. A written agreement may detail (taking into account the results of the information gathering exercise) requirements for the following aspects of sharing:

a) How shared data will be stored, accessed and used.

b) An agreed security classification for the shared data.
c) Suitable technical and organisational measures to protect data from accidental or unauthorised disclosure or misuse.
d) A requirement that permission be sought from the disclosing partner prior to any onward disclosure from the recipient of all or part of a bulk dataset or any targeted data derived from it.
e) A requirement that permission be sought from the disclosing partner prior to any executive action being undertaken by the recipient on the basis of any shared data or targeted data derived from it.
f) A requirement that disclosure of and access to any shared data be limited to appropriately cleared personnel within the recipient who have a business justification for access to the data.
g) All staff within the recipient with access to the shared data will be made aware of the provision governing the retention and examination of the shared data made within the written agreement.
h) A requirement for the destruction of the shared data as soon as its retention is no longer deemed to be necessary or proportionate.
i) A requirement to inform the disclosing partner of any threat to life reporting obtained from examination of the shared data.
j) An assessment that the sharing of data complies with the disclosing partner's legal obligations and that the receipt of the data by the receiving partner complies with their legal obligations.

Stage 3 – Individual consideration of each bulk dataset to be shared and the terms of handling instructions to accompany each bulk dataset shared

87) In every instance where sharing of bulk data were proposed then there would need to be particular consideration of that proposed sharing, having regard to the terms of any sharing agreement in place. In each case where a bulk dataset were shared with a partner, specific handling instructions would accompany it. In addition, insofar as considered appropriate, MI5 would require the recipient to apply specific safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements appropriate to the nature of the data being shared.

Stage 4 – Review

88) Were sharing of bulk data to occur, MI5 would maintain the following ongoing obligations:

a) Undertake reviews to ensure the necessity and proportionality case for sharing continued to exist.

b) Undertake reviews of the adequacy of the arrangements governing the sharing with each recipient, including Action On, as and when necessary.

c) End current sharing with a recipient if judged necessary as a result of the above.

d) Inform the recipient of any changes to MI5's legal obligations impacting on bulk data sharing and update, as necessary, any written agreements and/or handling instructions.