

Witness: GCHO Witness

Party: 3rd Respondent

Amended Number: 2

Exhibit: GCHO 3

Date: 06/03/17

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
- (2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
- (3) GOVERNMENT COMMUNICATION HEADQUARTERS
- (4) SECURITY SERVICE
- (5) SECRET INTELLIGENCE SERVICE

Respondents

AMENDED WITNESS STATEMENT OF GCHO WITNESS

I, GCHO WITNESS, Deputy Director in the Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

- 1) I am Deputy Director Mission Policy at GCHQ. In that role, I am responsible for drawing up the operational policies that underpin GCHQ's intelligence gathering activities and for ensuring that they are complied with. I have been in this role since 5 January 2015, having previously served as Deputy to my predecessor. I have worked for GCHQ in a variety of roles since 1997.
- 2) I am authorised to make this witness statement on behalf of GCHQ. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
- 3) Documents referred to as exhibited to this statement are attached as Exhibit 'GCHO 3'.

- 4) Further to paragraph 95 of the Investigatory Powers Tribunal's judgment of 17 October 2016 and paragraph 4 of the Tribunal's order of 31 October 2016, I make this statement in order to:
- a) exhibit (for the convenience of the Tribunal) relevant sections of policies/handling arrangements relating to the sharing of BPD and BCD;
 - b) address the question as to whether GCHQ has, since avowal on 11 March 2015, shared bulk personal data ("BPD") (or a sub-set of BPD) with international partners and/or law enforcement agencies ("LEAs"), and if so, what restrictions as to transfer or use/retention were imposed by GCHQ; and
 - c) address the question as to whether GCHQ has, since avowal on 4 November 2015, shared s.94 bulk communications data ("BCD") (or a sub-set of BCD) with international partners and/or LEAs and if so, what restrictions as to transfer or use/retention were imposed by GCHQ.

A. GCHQ'S POLICIES AND HANDLING ARRANGEMENTS RELATING TO THE SHARING OF BPD AND BCD

- 5) I exhibit the following as exhibit GCHQ.3:
- a) Paragraph 16 of the Joint SIA BPD policy of Feb 2015;
 - b) Paragraph 5.2 (4th bullet), paragraphs 6.0-6.7 and paragraphs 8.1 of the cross-SIA BPD OPEN Handling Arrangements of November 2015;
 - c) Section 9 of the GCHQ CLOSED BPD Handling Arrangements;
 - d) Paragraphs 4.4.1 to 4.4.6 of the OPEN Handling Arrangements for BCD; and
 - e) Section 4.4 of the GCHQ CLOSED s94 Handling Arrangements.
 - f) Raw Data Release Request Form

B. SHARING OF BPD/BCD WITH INTERNATIONAL PARTNERS AND LEAs

- 6) Where members of foreign intelligence agencies are posted to GCHQ as liaison officers they are not given access to any of GCHQ's operational systems.
- 7) Were members of foreign intelligence agencies to be posted to GCHQ as integrated staff then they would be required to agree that they would comply with the same policies and safeguards that GCHQ employees are required to comply with. Were GCHQ to make any of its BPDs available to integrated staff from liaison partners and/or law enforcement agencies, or to grant access to systems containing BCD, GCHQ would require analysts to have completed all relevant training (including legalities training which would be required to be in date), to be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances. All queries would be accompanied by necessity and proportionality statements which would be audited by GCHQ. Analysts would be required to comply with GCHQ's Compliance Guide and other BPD/BCD policies and safeguards concerning access, retention and use. The treatment of LPP and journalistic material would be addressed in the required training, and as set out in the Compliance Guide. Such safeguards would put partner analysts on the same basis as GCHQ analysts.

- 8) Were GCHQ to grant access to any of its systems or databases containing BPD or BCD to international partners from their premises, it would be on the basis that all analysts given accounts on the system or database would have completed all relevant training, including in-date legalities training, and that they were assessed as having sufficient analysis skills together with all necessary nationality and security clearances. All queries would be required to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ. Analysts would be required to comply with GCHQ's Compliance Guide (which addresses *inter alia* the treatment of LPP and journalistic material) and all other extant BPD/BCD policies and safeguards concerning access, retention and use.
- 9) Whilst we can neither confirm nor deny whether the SIA have agreed to share or in fact do share BPD/BCD with either foreign liaison partners or LEA, were we to do so, we would
- Follow the principles and approach set out in our respective Handling Arrangements and policy/guidance.
 - Take into account the nature of the BPD and BCD that was due to be disclosed.
 - Take into account the nature/remit of the body to which we were considering disclosing the BPD/BCD.
 - Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed.
 - Depending on the individual circumstance, seek assurances that the BPD/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).
 - If relevant to the particular circumstance, seek assurances that its use was in accordance with the UK's international obligations.
 - 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 Agencies.
- 10) 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 partners 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.

- 11) 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.

C. SHARING OF BPD/BCD WITH INDUSTRY PARTNERS

- 12) BCD/BPD may be shared with industry partners where necessary for the purposes of developing and testing GCHQ's operational systems. Industry partners are required to specify the controls that they intend to apply in relation to retention, use, examination and destruction. These controls are subject to approval before sharing. The approval process is set out in a request form attached as Exhibit 'GCHQ 3'. It should be noted that this form is also used to seek approval for the sharing of certain non BPD/BCD data in specific circumstances.
- 13) GCHQ may share operational data (which might in principle include BPD/BCD) 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.
- 14) All sharing of data with industry is recorded on a Raw Data Release Request form (exhibited at Exhibit GCHQ3) 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 or 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.

Statement of Truth

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

SCRCQ Witness

Dated: 6 March 2017

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

EXHIBIT GCHQ 3

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

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

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

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

D. Sharing

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

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

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

E. Retention

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

7.0 Review of Retention and Deletion

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

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

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

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

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

8.0 Other management controls within the Intelligence Services

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

discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective.

8.2 The Review Panel in each Intelligence Service meets at six-monthly intervals and are comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

8.3 Use of bulk personal data by staff is monitored by the relevant audit team in each Intelligence Service in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution.

8.4 All reports on audit investigations are made available to the Intelligence Services Commissioner for scrutiny (see paragraph 10 below).

8.5 Staff within each Intelligence Service will keep their senior leadership (at Director level or above) apprised as appropriate of the relevant Service's bulk personal data holdings and operations.

For the purposes of management control:

- ❖ A Review Panel in each Intelligence Service must meet at six-monthly intervals to review that Intelligence Service's BPD holdings.
- ❖ Staff must keep senior leadership (Director level or above) apprised of BPD holdings and operations.

9.0 Ministerial Oversight

9.1 Each Intelligence Service will report as appropriate on its bulk personal data holdings and operations to the relevant Secretary of State (the Home Secretary in the case of the Security Service, and the Foreign Secretary in the case of SIS and GCHQ).

10.0 Oversight by the Intelligence Services Commissioner

10.1 The acquisition, use, retention and disclosure of bulk personal datasets by the Intelligence Services, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.

Note: The Prime Minister's section 59A RIPA direction was issued on 11 March 2015. Paragraph 3 of this makes it clear that the Commissioner's oversight extends not only to the practical operation of the Arrangements, but also to the adequacy of the Arrangements themselves.

10.2 The Intelligence Services must ensure that they can demonstrate to the appropriate Commissioner that proper judgements have been made on the necessity

OFFICIAL

7.8 In the case of systems containing operational data, specific details of individuals' activities while accessing the system are logged and are subject to audit. Such logs contain details of who was accessing the system, when, and what they did while logged in. Users are also required to provide a Necessity & Proportionality Statement ("N&P Statement") for conducting an analytical search of the data in the system; an N&P Statement consists of a statement of the operational purpose of the search and an explanation of its necessity and proportionality. These justifications are also logged and are subject to periodic audits of their legitimacy and adequacy.

7.9 GCHQ's Legal and Policy training includes a section on N&P Statements. More detailed guidance on how to formulate legitimate and adequate justifications is available to all staff via links from GCHQ's Compliance Guide.

8. Experimental Use

8.1 Use of bulk personal data for an experimental purpose, e.g. development of a novel analytical technique or testing a new IT system, potentially entails an elevated level of risk to the security of the data, increased corporate risk and an additional interference with the right to privacy.

8.2 Any proposed experimental use of a bulk personal dataset must be authorised in advance by the relevant GCHQ senior officials. A request for authorisation will be made, using the relevant section of the dataset's BPD form. It will describe the proposed activity and explain why it is necessary and proportionate to use bulk personal data for this purpose. It will also include an assessment of the impact the experimental use is expected to have on the risks and interference mentioned above.

8.3 The Authoriser will consider the necessity and proportionality of the proposed use, in particular whether it is genuinely necessary to use bulk personal data for this purpose, given its intrusiveness and the degree of corporate risk involved.

8.4 If the request to use the bulk personal dataset for the proposed experimental purpose is approved, the Authoriser may, at his/her discretion, set conditions or restrictions on its use. If the request is rejected, the dataset must not be used for that purpose. The decision and any conditions or restrictions must be recorded on the dataset's BPD form.

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:

9.3 Another SIA Agency:

9.3.1 If the proposed recipient of the dataset is another SIA Agency, that Agency will (as with any other operational data) formally request transfer of the data via the "Inter-Agency Sharing" (IAS) process. As with authorisation to acquire a bulk personal dataset, this disclosure request will be considered and authorised (or rejected) by relevant GCHQ senior officials. The Authoriser's decision and the reasons for it will be recorded on the dataset's BPD form, as well as on the IAS request form.

OFFICIAL

6 of 10

OFFICIAL

[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.

[REDACTED]

10. Continued Retention

10.1 The ongoing retention of every bulk personal dataset is reviewed at least every 24 months by the Bulk Personal Data Retention Review Panel (the Panel).

10.2 The Panel consists of relevant senior GCHQ officials.

10.3 Representatives from MI5 and SIS are normally invited to observe and contribute to discussions.

10.4 The Panel meets every 6 months, typically in March and September, to consider the datasets due for review and to review the functioning of the bulk personal dataset life-cycle management processes. Discussions, decisions and actions are minuted.

10.5 If a dataset's Requester and Endorser consider that a convincing case can be made to justify the continued retention and exploitation of that dataset, they must submit a retention request to the Panel by means of the dataset's BPD form. If they do not believe a convincing case can be made, they must arrange for the deletion of the dataset as soon as they reach this conclusion.

10.6 In the request, they must justify the interference with the right to privacy caused by GCHQ's continued retention and exploitation of the dataset. They must set out why it is genuinely necessary and proportionate to continue to retain and use the data. This rationale must be supported by concrete evidence, including specific examples, where possible, of the

OFFICIAL

7 of 10

and vetting regime for staff.

- ❖ Limit access to those with appropriate business requirement.
- ❖ Justify access to BCD on the grounds of necessity and proportionality, taking into consideration collateral intrusion and other less intrusive methods of deriving the same intelligence dividend.
- ❖ Ensure staff are appropriately trained, aware of audit functions and warned of disciplinary procedures resulting from misuse.

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 Official² 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

² Equivalent to a member of the Senior Civil Service.

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

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

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

Disclosure of BCD must be:

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

4.5 Review of Ongoing Acquisition and Retention, and Deletion

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

4.5.2 The retention and review process requires consideration of:

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

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

[REDACTED]

4.3.15 All records of searches and queries, together with the accompanying N&P statements, are centrally logged and are subject to periodic audits of their legitimacy and adequacy. Records relating to section 94 data and related communications data may be inspected by the Interception of Communications Commissioner.

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.

4.4.3 If the proposed recipient of the dataset is another SIA Agency, that Agency will (as with any other operational data) formally request transfer of the data via the "Inter-Agency Sharing" (IAS) process. As with authorisation to acquire section 94 data, this disclosure request will be considered and authorised (or rejected) by the relevant GCHQ senior officials. The Authoriser's decision and the reasons for it will be recorded on the IAS form.

[REDACTED]

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.

[REDACTED]

4.5 Data Retention, Review and Deletion

[REDACTED]

4.5.3 A Review Panel conducts a comprehensive review of GCHQ's section 94 data, and of the directions used to acquire the data, at six-monthly intervals. The review determines

8 of 8

[REDACTED]

OFFICIAL

REQUEST TO RELEASE RAW DATA
[REDACTED] TO INDUSTRY PARTNERS

Updated Sept. 2016

NAME and TEAM OF REQUESTOR:

DATE OF REQUEST: / /

POLICY RESPONSE REQUESTED BY: / /

Who do you want to release the data to?	
[REDACTED]	[REDACTED]
[REDACTED]	INDUSTRY
[REDACTED]	

[REDACTED]

ON COMPLETION, THIS FORM SHOULD BE EMAILED to:

[REDACTED]

For sharing with Industry please send to GCHQ Policy team.

1 of 5

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq

OFFICIAL

SUMMARY		
What data do you want to release? (Please include type of data e.g. [REDACTED]. Please include <u>technical details</u> .)		
Will this be a one-off, repeated or ongoing requirement?		
Please provide context details on the [REDACTED] project		
Why do you want to send the data? (Please provide clear business benefit, where applicable include <u>justification</u> and statutory purpose NS/SC/EWB where relevant). What are the expected outputs? Is there any precedent for this request? (If so, please provide details)	National Security	Economic Well-Being
	Serious Crime	

OPERATIONAL DATA	
How much data is needed to complete the task?	
Is the data selected or non-selected?	
What is the Protective Marking / Classification of the data?	
Is the data owned by GCHQ? (If the data is not owned by GCHQ please identify the owner, and include <u>technical details</u> where possible. If owned by a collaborating agency, please state which agency.)	
Will the identity of SIGINT targets be apparent in the data? If so is there an <u>internal approval form</u> relevant to the targets? -- if so please provide details	
Will the means by which GCHQ has acquired the data be apparent to the recipient?	
Has the data been processed by [REDACTED]? If yes, please include formal release approval (email) from <u>relevant team</u> .	
Is the data from [REDACTED]? If yes, please include formal release approval (email) from <u>relevant team</u> . [REDACTED]	

OFFICIAL

RECIPIENTS' DETAILS	
	Who will the data be provided to? (Please provide organisation, name and job title.)
	How many additional people will require access to the intercept and where are they from?
	Please provide the level of clearance and indoctrination (SC, DV, STRAP etc.) for all recipients mentioned above.
	[REDACTED] Please include details of any [REDACTED] briefings required/received
	What is their employment status within their organisation (employee, contractor etc.)?
	Where will the data be processed? [REDACTED] Industry partner and IT system(s) (Please include details of system accreditation levels and additional security measures in place to protect the data, how classification will be implemented and provenance details retained)
	How will the data be sent there? (Please include details of secure transfer method to be used)
	How long will the data need to be kept to complete the task?
	Will the data be destroyed or returned to GCHQ? (Please include details of destruction processes in place if not being returned)

4 of 5

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq

OFFICIAL

OFFICIAL

ANY OTHER CONSIDERATIONS?

ADDITIONAL DETAILS (FOR APPROVERS USE ONLY)

AUTHORISED BY: (NAME AND DATE TO BE COMPLETED BY GCHQ POLICY TEAM OR (REDACTED)) PLEASE INCLUDE ANY ADDITIONAL CAVEATS/CONDITIONS FOR APPROVAL IN YOUR RESPONSE The approver should save the form with the approval / rejection decision to <i>corporate document and records management system</i> .

5 of 5

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01 242 221491 x30306 (non-sec) or email infoleg@gchq

OFFICIAL

