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

SIA Bulk Personal Data Policy

[REDACTION]

SIA Bulk Personal Data Policy

v.1 February 2015

- A. General
- B. Acquisition
- C. Use
- D. Sharing
- E. Retention
- F. Deletion/Destruction
- Annex A

A. General

Introduction

1. The policy and legal environment which governs our use of bulk personal data is changing fast. The ground shifted significantly with the Prime Minister's decision earlier this year to avow publicly SIA use of bulk personal data, oversight arrangements and a safeguards regime. This was all in the context of the imminent publication of the ISC's report on privacy and security (the catalyst for the avowal), not to mention David Anderson's investigatory powers review, which was published on Thursday 11 June. The sharp increase in the political profile of bulk data was only too apparent to those parts of MI5 administering our bulk data holdings, with the need to forewarn each data provider that avowal was going to take place. But other parts of MI5, including bulk data users, perhaps felt this less.

2. Post the election, the new government is now considering changes to our powers and oversight – so-called 're-licensing' – in the light of the ISC and Anderson reviews. As part of this, the SIA use of bulk personal data may become subject to more onerous authorisation processes (beyond our current largely internal ones), as well as enhanced external oversight. At the very least we should expect increased and significant public interest and debate. Indeed, as of Monday 8 June, the Investigatory Powers Tribunal received a challenge to the SIA's use of bulk personal data from Privacy International following ISC avowal. Further

scrutiny and debate will follow.

3. In this context we need to be exemplary in the way we operate our existing processes for bulk personal data. This falls on each and every one of us. Below we describe what we all need to do.

4. This document sets out SIA (GCHQ, MI5 and SIS, or 'the Agencies') policy in relation to Bulk Personal Data (BPD), as agreed by all three Agencies. It aims to assist staff involved in all aspects of BPD Lifecycle and its Oversight. Each Agency has developed separate, Agency specific guidance for its staff aligned with this policy to assist with managing its own BPD Lifecycles. The Agencies have aligned specific business processes where appropriate to allow for greater co-operation and consistency of approach.

These boxes will appear throughout the policy to highlight areas where the SIA wide agreements have been built upon to assist staff working with BPD in MI5.

Definition of 'Bulk Personal Data'

5. The Agencies lawfully collect a range of information from a variety of sources which is needed to meet their statutory functions in an effective and timely manner. The data collected includes datasets which contain personal data about a wide range of individuals, the majority of whom are not of direct intelligence interest. These datasets are known as Bulk Personal Datasets and are acquired via various statutory gateways (see Annex A for explanation of statutory gateways and oversight arrangements). They share the following characteristics;

- Contain personal data about individuals, the majority of whom are unlikely to be of intelligence or security interest;
- Are too large to be manually processed (particularly given benefit is derived by using them in conjunction with other datasets);
- Are held on analytical systems within the SIA.

6. In this context, 'Personal Data' has the meaning given to it in section 1(1) of the Data Protection Act (1998) (DPA) which defines 'personal data' as follows;

'data which relate to a living[1] individual who can be identified –

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of the data controller (i.e. the relevant Agency), 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'.

7. Similarly, the definition of 'Sensitive Personal Data' has the meaning given to it in the DPA (1998), and so covers the following;

- Racial or ethnic origin;
- Political opinions;
- Religious belief or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual life;
- The commission or alleged commission of any offence; or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

SECURITYSERVICE MI5

MI5 considers for internal handling purposes the following should be regarded as being within the category of 'sensitive personal data' (using this term in a non-statutory sense):

- biometric data,
- related to a Member of Parliament,
- about journalists,
- financial,
- employment within the SIA,
- information that is operationally sensitive to the SIA,
- information subject to legal professional privilege.

BPD must be categorised to aid their management and to allow for greater clarity in external communications and briefings. Please see separate guidance for the description of MI5 current categories.

8. In addition to the DPA-defined statutory categories, each Agency may have additional policies (with additional controls) in which they define further categories as 'Sensitive Personal Data' (in a non-statutory sense). In practical terms, this means the Agencies recognise and may, as judged appropriate, take additional steps to protect data relating to these subjects.

Managing Bulk Personal Data

9. Each Agency must have arrangements in place for the effective management and legal compliance of BPD throughout its lifecycle. The stages of the BPD lifecycle are:

- Acquisition – the initial authorisation processes, arrangements for collection, receipt, storage and loading of BPD onto Agency systems;
- Use – access to, and use of, the data by Agency staff, authorisations required for different types of use, reviews of use, safeguards;
- Sharing – ***sharing of data with partners***, authorisations, reviews of use;
- Retention – ensuring Agencies do not retain data longer than is necessary, review processes;
- Deletion/Destruction – decision making, processes to ensure effective, recording and confirmation of the deletion/destruction.

10. This policy document describes and prescribes the arrangements common across the three Agencies. Separate Agency-specific guidance is published by each of the Agencies to

interpret the policy on the basis of individual Agency needs.

Governance

11. Each Agency must have a governance structure and a process in place to ensure effective oversight of the BPD lifecycle. These governance structures must provide robust frameworks to ensure each Agency handles its information appropriately and in compliance with the law.
12. These structures support the Head of each Agency in the discharge of their statutory duties as the individual with overall responsibility for obtaining and retaining the Agency's information, and assist them in managing associated risks.

13. Each Agency must have a review panel whose function is to oversee the lifecycle of the BPD it holds. The composition and specific processes may vary between the Agencies, but each must be chaired at senior (director or deputy or assistant director – as appropriate for each Agency) level, and include, legal advisers, technical teams, compliance or policy teams and representatives from the business as judged appropriate. Invitations should also be extended to each of the other two Agencies.

SECURITYSERVICE MI5

MI5 reviews the operational and legal justification for the continued retention of bulk personal datasets through the Bulk Personal Data Review Panel (BPDR Panel), chaired by ***a senior MI5 official.***
The aim of the Panel is to ensure BPD has been properly acquired and its retention remains necessary and proportionate to enable the Service to carry out its statutory duty to protect national security. Panel members must satisfy themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR and is in line with the requirements of the Data Protection Act 1998

External Oversight

14. Bulk Personal Datasets (as defined above) are acquired under a variety of statutory gateways. It is important to distinguish between these gateways for the purposes of oversight by the respective Commissioners. The full legal rationale aligning acquisition gateways and the respective oversight arrangements is at Annex A, but can be summarised in the table below:

	Legislative Gateway	Oversight by
1a	Security Service Act s.2(2)(a) Intelligence Services	Intelligence Services

	Act s.2(2)(a) (for SIS) and s.4(2)(a) (for GCHQ) (voluntary supply and other non-covert access methods) Counter Terrorism Act s.19(1) and 19(6)	Commissioner (non-statutory)
1b	Intelligence Services Act s.5 (property warrants), RIPA Part 2 s.28 (directed surveillance), s.29 (CHIS) and s.32 (intrusive surveillance)	Intelligence Services Commissioner (statutory)
2a	Telecommunications Act s.94	Interception of Communications Commissioner (non-statutory – once formally established)
2b	RIPA Part 1, Chapter 1 (intercept), RIPA Part 1, Chapter 2 (communications data)	Interception of Communications Commissioner (statutory)

SECURITYSERVICE MI5

The purpose of this oversight is to review and test our judgements on the necessity and proportionality of acquiring and using bulk personal datasets and to ensure our policies and procedures for the control of, and access to, these datasets is both sound and strictly observed. Although we brief the Home Secretary on MI5's use of these techniques, independent oversight by the Intelligence Services Commissioner provides a third party view of the arrangements that have been agreed. It also affords an independent view on our judgements that provides assurance to both MI5, the Home Secretary and the Prime Minister.

The oversight team coordinate the Commissioners visits and ***the data governance team*** must provide copies of a high- level summary of MI5's BPD holdings, alongside individual copies of the retention forms and the decisions made. Any 'Need To Know' datasets must be provided by the data sponsor directly to the oversight team. Additional papers requested by the Commissioner must be made available to them.

The Home Secretary is informed annually of BPD use within MI5 via the Operational Policies document.

B. Acquisition

15. The acquisition of BPD is controlled tightly. The following policy statements apply to the

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

Agencies:

- All acquisition must be authorised by a senior manager within the Agency (specific arrangements vary between Agencies);

SECURITYSERVICE MI5

Within MI5, this role is the responsibility of senior MI5 officials.

- Where a request is made to obtain a dataset it must be justifiable and deemed necessary and proportionate for the requesting Agency to acquire the dataset in pursuit of its statutory functions;
- The acquisition of BPD must be authorised before any analytical exploitation of the data. Authorisation may need to be obtained at an earlier stage at the individual Agency's discretion. If authorisation is not granted the relevant BPD must be deleted;

SECURITYSERVICE MI5

Importantly the acquisition of BPD in MI5 must be authorised prior to acquisition. Failure to adhere to this MI5 policy and failure to follow the MI5 guidance may result in disciplinary action being taken and must be reported to ***the relevant team*** as soon as such behaviour is identified.

In determining whether to grant an authorisation, a justification of the necessity and proportionality, is submitted by a senior manager from the requesting business area. This is also scrutinised by a legal advisor and the ***relevant team*** before a decision is taken. ***A senior MI5 official in the ethics team*** can also be consulted at any stage of the process

The legal advisors play an important part in this process, providing a legal view on the acquisition of BPD by MI5, which must be in accordance with the law.

- All BPD will be assessed to determine the levels of Intrusion and Corporate Risk during the acquisition process. These considerations will assist in the decision regarding the review periodicity for the dataset;
- [REDACTION]
- It is the responsibility of the Agency that acquired the data to manage the relationship with the data supplier. Where an Agency shares a dataset with another, the receiving Agency is responsible for its copy. If the acquiring Agency decides to delete/destroy the dataset but the other Agencies wish to retain the data and have sufficient justification, the Agencies must agree between them the responsibilities for managing supplier equities, source, and/or technique protection. As judged appropriate, this may involve the transfer of responsibility for managing the relationship, source or capability to one of the other Agencies, or the continued supply of data by one Agency on behalf of the others;
- All BPD sets held within and shared between the SIA must have a clearly identified lead Agency;
- The Agencies will co-ordinate to ensure efficiency in the acquisition of BPD. This includes de-confliction to prevent parallel or duplicative acquisition;
- [REDACTION]
- After receipt of BPD there must be robust access controls constrained to those with a business need, to all versions of information held on any medium/system;
- [REDACTION]

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

SECURITYSERVICE MI5

The acquisition of BPD by MI5 is subject to internal scrutiny by a specific team within MI5. There are standard processes which MI5 officers must follow in order to acquire BPD which are outlined in separate guidance.

C. Use

16. The use of BPD is managed and monitored to ensure the principles of necessity and proportionality are followed thereby enabling the Agencies to fulfil their statutory requirements. The following policies apply to the use of BPD:

- The Agencies must; consider the different levels and types of intrusion and the sensitivities inherent in the exploitation of BPD; ensure that BPD is hosted and available on suitable analytical systems; and ensure that appropriate safeguards are in place to prevent and detect inappropriate use;
- [REDACTION]
- Access to analytical systems which have the ability to interrogate BPD must be restricted to those with a business need and have an appropriate level of security clearance;
- Users must complete relevant training and be made aware of their responsibilities (in relation both to the analytical systems and the data they access) before they are granted use of analytical systems which can interrogate BPD. In exceptional circumstances if an individual has not completed the relevant training and a strong business case exists for their use of analytical systems containing BPD then their use of these systems must be guided by an experienced trained colleague;
- Each Agency must ensure all use of BPD, in whatever context, is necessary and proportionate to enable the Agency to fulfil its statutory obligations, and that use must be authorised at an appropriate level commensurate with the use proposed, level of intrusion, and assessment of risk;
- Users must ensure their queries against BPD are structured and focused so as to minimise collateral intrusion;
- BPD may be used to conduct experiments as part of the SIA drive to improve data analytics, however the risks arising from use in an experiment must be considered and pre-authorised by a senior manager;

SECURITYSERVICE MI5

Within MI5, ***a senior MI5 official*** has the responsibility of authorising the use of BPD in experiments. The use of BPD should be excluded by default from experiments and only included by exception.

- Physical, technological and administrative safeguards must be in place to guard against the misuse, malicious or otherwise, of BPD and the analytical systems upon 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.

D. Sharing

17. 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;

Within MI5, the sharing of BPD is authorised by ***a senior MI5 official.*** This decision requires the input of a legal advisor to ensure the disclosure is in accordance with the law.

- [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.***

There are standard processes within MI5 which sections must follow in order to share BPD which are outlined in separate guidance.

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;
- Each Agency must provide its own justification for the retention of a dataset. Where an Agency shares a dataset with another, the receiving Agency is responsible for its copy;
- Different Agencies may reach different conclusions about the value of, and requirement to retain (or delete) the same dataset, based on each Agency's ongoing business

requirement, and assessment of risk, necessity and proportionality;

- If the acquiring Agency chooses to delete a dataset, the consequences for retention must be considered by all Agencies with access to that dataset. If the other Agencies wish to retain their copy and have sufficient justification, the Agencies must also agree between them the responsibilities for managing supplier equities, source, or technique protection. As judged appropriate, this may involve the transfer of responsibility for managing the relationship, source or capability to one of the other Agencies, or the continued supply of data by one Agency on behalf of the others;
- All decisions on retention (either full or partial) must be recorded;
- The frequency of retention reviews for BPD varies across the Agencies, but all are periods determined by similar factors, including potential use (or lack of); levels of intrusion; and levels of sensitivity/corporate risk;
- The level of use and Intrusion and Corporate Risk for a BPD must be re-assessed during the review process;
- The review period assigned to a dataset can be altered if an acceptable justification can be made. Such changes must be authorised by the review panel and the justification recorded.

SECURITYSERVICE MI5

For MI5, the Bulk Personal Dataset Review Panel (BPDRP) is responsible for the oversight described above and it shall be the responsibility of ***the relevant team*** to coordinate this activity. The review of BPD retention must be captured on ***the appropriate form.***

The frequency of review period for retention and disposal of a dataset is determined by the lesser time period in either;

i. The assessed levels of Intrusion and Corporate Risk for the dataset; Or
ii. Any Retention, Review and Disposal (RRD) specific Handling Arrangements relevant to the dataset.

All BPD must be assessed for levels of intrusion and corporate risk at the acquisition of the dataset and each subsequent review. Please see separate guidance on assessing intrusion and corporate risk. Where a review period is determined by the levels of intrusion and corporate risk (and not specific handling arrangements) the following review period is assigned:

Review Category	Intrusion	Corporate Risk	Review Period
Category 1	High	High	6 months
Category 2	Medium	Medium	1 Year
Category 3	Low	Low	2 Years

Where the assessed levels of intrusion and corporate risk differ then the review period is

determined by the shorter time period. Other factors may be considered when determining the review period of a dataset such as its use. The review period assigned to a dataset can be altered (either up or down) if an acceptable justification can be made. These changes must be authorised by ***a senior MI5 official*** and agreed by the BPDRP.

In MI5 a maximum retention period [REDACTION] is applied to the retention of BPD. This can be increased in exceptional circumstances via a policy waiver. This waiver must be authorised by ***a senior MI5 official*** and agreed by the BPDR Panel but shall be subject to a detailed review. A dataset shall be excluded from such additional scrutiny where:

- ***The review period*** is deemed inappropriate by the Panel

Any alternative retention rules agreed under a policy waiver shall be detailed on ***the relevant form.*** In subsequent reviews, the data sponsor must confirm whether those deletion requirements are still appropriate.

F. Deletion/Destruction

19. It is a legal requirement for the Agencies not to hold BPD for longer than is deemed necessary and proportionate. The following policy statements apply to the disposal of BPD:

- The review panel will instruct the deletion/destruction of BPD when they are no longer necessary and proportionate. BPD will not be archived unless there is a legal justification such as disclosure;
- If the primary acquiring Agency has to delete a dataset (e.g. following Commissioner intervention, or at the request of a data supplier) and one or both of the other Agencies decide to retain the data, the other Agencies must also review their justification for retention of the same dataset. The standard of justification for any ongoing retention in such circumstances is likely to be high;
- If one or both of the other Agencies decide to retain the data, the Agencies must agree between them the responsibilities for managing the data [REDACTION];
- Where a dataset is to be deleted/destroyed by an Agency it must consider ***any previous sharing*** of the data with liaison partners (e.g. ***foreign agencies***, police, OGDs). Depending on the circumstances surrounding the deletion/destruction, a decision must be made as to whether to ask third parties to delete/destroy their copy or extract of the dataset. If the decision is to request deletion, the request must be made even if there is little prospect of being able to enforce deletion/destruction by the third party;
- The review panel can request the deletion/destruction of certain fields/criteria from within a dataset if they are not deemed to be necessary and proportionate whilst retaining the remainder of the dataset;
- The Agencies' relevant technical sections are responsible for conducting the deletion/destruction of the dataset [REDACTION]

Within MI5, if data is no longer required, then the relevant data sponsor must request its deletion at that point, and not wait for the next review. The BPDRP may also request a dataset

should be deleted either partially or in its entirety.

Once deletion and destruction activities are completed, the relevant technical section is responsible for notifying ***senior MI5 officials*** this has been completed in accordance with the relevant MI5 policy and guidance. ***Senior MI5 officials*** will track deletions and submit an update to the next BPDRP.

Annex A

Bulk Data: Oversight Arrangements - Note to accompany 'Definition' document

(A) The Intelligence Services Commissioner

The bulk personal datasets scrutinised by the Intelligence Services Commissioner under the current non-statutory arrangement comprise those bulk personal data sets that are usually (though not exclusively) acquired - at any rate, by MI5 - under section 2(2)(a) of the SSA. This oversight was put in place to cover a gap in oversight as well as to provide some assistance in addressing [REDACTION] Article 8 'foreseeability' [REDACTION] in relation to bulk personal datasets acquired by MI5 under section 2(2)(a) of the SSA, and by SIS and GCHQ under section 2(2)(a) and section 4(2)(a) respectively of the ISA (the "information gateway provisions").

Although the majority of the bulk personal datasets acquired by MI5 have been acquired under section 2(2)(a) of SSA, this is not necessarily the position in relation to SIS or GCHQ. And, recently, MI5 has acquired bulk personal datasets falling within the above definition using intrusive powers under Part 2 of RIPA (ISWs, DSAs and CHIS authorisations) and under section 5/ISA (property warrants), and this trend may increase in the future.

The Counter-Terrorism Act 2008 (CTA) provides individuals, companies and public authorities (including other government departments) with a clear legal basis for providing data to MI5, where it is necessary and proportionate for the proper performance by the Service of its statutory functions, including that of protecting national security. Section 19(1) of the CTA provides that any 'person' may lawfully disclose information to the Security Service for the purposes of the Service's exercise of its statutory functions. Section 19(6) of the CTA disapplies any duty of confidence or any other restriction which might otherwise have prevented such a disclosure taking place. This framework ensures that disclosures to MI5 are lawful and provides an environment which facilitates the acquisition and sharing of BPD where the Security Service's statutory functions are engaged.

Since the exercise of such powers falls within the statutory oversight remit of the Intelligence Services Commissioner, it makes sense for any bulk personal datasets acquired in the

exercise of such powers also to be scrutinised by the Intelligence Services Commissioner - in the same way that he oversees bulk personal datasets acquired under section 2(2)(a) of SSA.

We also consider it makes sense for the internal "section 2(2)(a) bulk personal data authorisation process" to be applied in parallel to the necessary RIPA Part 2/section 5/ISA authorisations in situations where the express intention is to collect a bulk personal dataset falling within the definition above. As a general rule, of course, the vast majority of individually targeted RIPA Part 2 and section 5/ISA authorisations will not be aimed at obtaining a bulk personal datasets and so will not fall to be dealt under the s. 2(2)(a) bulk personal data authorisation arrangements, which means that the use of parallel authorisations should be minimised.

Moreover, acquisition of all the above datasets is required to be in accordance with the provisions of section 2(2)(a) of the SSA and the corresponding "information gateway provisions" applicable to SIS and GCHQ. These provisions impose a duty on the Heads of the respective Agencies to ensure that there are arrangements for securing (i) that no information is obtained by the relevant Agency except so far as necessary for the proper discharge of its functions (and, in the case of the Secret Intelligence Service and GCHQ, for the purposes for which those functions are exercisable); and (ii) that no information is disclosed except so far as is in accordance with the disclosure gateways.

(B) The Interception of Communications Commissioner

It is axiomatic that any datasets which are acquired under other legislative gateways such as Part 1, Chapter 1 and 2 of RIPA, or under section 94 of the Telecommunications Act 1984, albeit that they may fall within the above definition, will not fall to be overseen by the Intelligence Services Commissioner. Nor, in general will they fall to be included in our respective internal bulk personal data authorisation process described in (A) above.

There may be rare circumstances where it is judged appropriate to run the bulk personal data authorisation process referred to in (A) above in parallel to a RIPA Part 1, Chapter 1 warrant application or Chapter 2 authorisation process, in situations where the intention is to collect data meeting the definition of 'bulk personal data'. The exceptional circumstances where - in relation to the collection of such bulk personal data under Part 1 Chapter 1 or Chapter 2 of RIPA - it may be appropriate to run the authorisation process referred to in (A) above in parallel, may include cases when intercept is used to capture a dataset which is not communications-related (e.g. financial transactions), or where an intercept runs for only a short period of time and retention of the dataset in question is required well beyond the termination of the interception warrant.

Whilst there is no legal requirement for such an arrangement, it may be judged good practice

and would help the SIA to manage data effectively and appropriately.

Section 57 of RIPA makes it clear that interception and communications data operations under Part 1 of RIPA are within the exclusive statutory oversight remit of the Interception of Communications Commissioner (IoCCO). Therefore, we propose that in such situations, oversight of the intercepted product or communications data acquired under RIPA Part 1, Chapter 1 or 2 – even where this is also subject to the parallel bulk personal data process referred to in (A) above - will remain with the Interception Commissioner.

In order to ensure consistent oversight of communications data management under the Interception Commissioner, it is also proposed that the Interception Commissioner should undertake non-statutory oversight of: datasets acquired pursuant to directions under section 94 of the Telecommunications Act 1984 (which will necessarily be communications data-related datasets).

(C) Oversight of Sharing of datasets originally acquired under RIPA Part 1, Chapter 1 and 2 (or section 94 Telecommunications Act directions)

With regard to IoCCO oversight, the question arises whether Part 1 RIPA oversight by the Interception Commissioner extends – or should extend – to datasets (or subsets of this material) which were acquired originally under Part 1, Chapter 1 and 2 of RIPA by another Agency (e.g. GCHQ), even if those datasets are subsequently acquired by say, MI5 or SIS under their respective 2(2)(a)/SSA/ISA gateways, or whether such oversight should fall to the Intelligence Services Commissioner.

There would be some logic from a policy perspective for IoCCO to take on oversight of all intercept-related and communications data- related datasets regardless. In the GCHQ example just given, GCHQ's disclosure of a bulk dataset comprising intercept product derived from its own interception activity would in any event be subject to the RIPA Section 15 Handling Arrangements, and so such disclosure by GCHQ would appear to be properly within the statutory oversight remit of IoCCO.

However, as the legal gateway for acquisition by MI5/SIS would be 2(2)(a) of SSA/ISA, to confer oversight of such acquisition on IoCCO rather than the Intelligence Services Commissioner would arguably muddy the water in what is an otherwise clear delineation between the two Commissioners by reference to the statutory gateway that is engaged.

Assuming that IoCCO takes on oversight of communications data-related datasets pursuant to directions under section 94 of the Telecommunications Act, a similar point will arise in relation to oversight of the acquisition by other Agencies of the relevant communications dataset under section 2(2)(a)/section 4(2)(a) from the originally acquiring Agency (which had acquired

pursuant to an IoCCO-overseen section 94 direction).

This point requires further consideration by the SIA. Given the unavoidable overlap that seems to arise in such cases where different statutory gateways are engaged, whatever approach we ultimately decide on will need to be brokered with the two Commissioners themselves.

1 Whilst DPA refers only to 'a living individual', many bulk personal datasets will contain details about individuals who are dead. SIA policy and processes in relation to bulk personal data is the same for both the living and the dead.