Home Office

Security and Intelligence Agencies' retention and use of bulk personal datasets

Draft Code of Practice Draft

[Spring] 2016

Security and Intelligence Agencies' retention and use of bulk personal datasets

DRAFT Code of Practice

Pursuant to section 207 and Schedule 7 to the Investigatory Powers Act 2016

[Spring] 2016

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Part 7 of the Investigatory Powers Act [2016] ("the Act"). It provides guidance on the procedures that must be followed before bulk personal datasets can be retained, examined and disclosed by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the Security and Intelligence Agencies"). This code of practice is intended for use by the Security and Intelligence Agencies.

1.2 The Act provides that all codes of practice issued under Schedule 6 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, it must be taken into account.

1.3 For the avoidance of doubt, the guidance in this code takes precedence over any Security and Intelligence Agency's internal advice or guidance.

2 Scope and definitions

2.1 The Security and Intelligence Agencies need to collect a range of information from a variety of sources to meet the requirements of their statutory functions. They do this in accordance with section 2(2)(a) of the Security Service Act 1989 (SSA) and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 (ISA) ("the information gateway provisions" – see paragraph 11.1 and subsequent paragraphs of Annex A) and through the exercise of various existing statutory powers (see further at paragraph 2.11 and subsequent paragraphs).

2.2 Among the range of information collected are bulk personal datasets ("BPDs"). For the purposes of the Act and this Code, a set of data comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.

2.3 Section 174 of the Act specifies that a Security and Intelligence Agency "retains" a BPD for the purposes of the Act if, after any initial examination of the contents, it retains a BPD for the purpose of the exercise of its functions; and it holds the BPD electronically for analysis in the exercise of those functions.

2.4 As section 190 makes clear, the initial examination enables the Security and Intelligence Agency, when it comes into possession of a BPD, to carry out a preliminary examination of the contents with a view to establishing whether it is a BPD, and that BPD is of a nature that the Security and Intelligence Agency would wish to retain and/or examine it. If so, the Security and Intelligence Agency will consider whether in the light of the dataset's potential intelligence or investigative value, it would be necessary and proportionate to retain the dataset for the purposes of analysis in the exercise of its statutory functions. If it concludes that it would be necessary and proportionate to retain the dataset for these purposes, that retention must be authorised by a BPD warrant. If the dataset is not covered by an existing class BPD warrant, the Security and Intelligence Agency must apply for a specific BPD warrant as soon as reasonably practicable after reaching that conclusion. (See chapters 3 and 4 for further details on these two types of BPD warrant.)

2.5 This initial examination may only be carried out by a Security and Intelligence Agency for these limited purposes, and not for the purposes of any intelligence investigations or operations.

2.6 A Security and Intelligence Agency should complete this initial examination as soon as reasonably practicable. What is 'reasonably practicable' will depend on many different factors. In cases where the Security and Intelligence Agency comes into possession of a BPD which has been created outside of the UK, there may be a period of time before the Security and Intelligence Agency is in a position to properly assess the data for the purpose of determining whether it wishes to retain or use the BPD (and to apply for a specific warrant, if required). For example, the BPD may need to be brought back to the UK from overseas; the BPD may be in a foreign language; and/or the BPD may be part of a much larger set of data from which it needs to be separated.

2.7 In the light of these considerations, section 190(4) specifies that in cases of BPD created outside of the UK, the acquiring Security and Intelligence Agency has six months from the date on which the head of the intelligence service believes a BPD has – or may have been - obtained to conduct the initial examination and, where required, to apply for a specific BPD warrant. Where the BPD is created in the UK, the acquiring Security and Intelligence

Agency has three months from the date on which the head of the intelligence services believes that a BPD has – or may have been - obtained to conduct the initial examination and where required apply for a specific BPD warrant.

2.8 Section 190(5) makes it clear that a Security and Intelligence Agency is not in breach of the requirement for a warrant to retain BPD for the period between deciding (as part of the initial examination) that it wants to retain a BPD and the determination of the Security and Intelligence Agency's application for a specific BPD warrant for that BPD. This allows a Security and Intelligence Agency which has received a BPD that falls outside an existing class BPD warrant to retain the dataset while going through the process of obtaining the necessary specific warrant. This is most likely to occur where a BPD is unsolicited (i.e. one which the recipient Security and Intelligence Agency has not requested or sought to obtain), because a Security and Intelligence Agency will not have had the opportunity to assess whether the BPD is covered by a class warrant. However, it could also arise where a solicited BPD is received which contains unexpected material. In such circumstances, the relevant Security and Intelligence Agency should complete its initial examination of the BPD and apply for a specific warrant within the timeframes referred to in section 190(4) (and described in paragraph 2.7 above). Pending issue of the specific warrant, the Security and Intelligence Agency may not examine the BPD for the purposes of any intelligence investigations or operations.

2.9 For the purposes of the Act, 'personal data' has the meaning given to it in section 1(1) of the Data Protection Act 1998 ("DPA" – see also paragraph 11.7 and subsequent paragraphs of Annex A), which defines 'personal data' as follows:

- 'data which relate to a living 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. in this case, the relevant Security and Intelligence 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'.

2.10 While the DPA refers to a 'living individual', bulk personal datasets may contain details about individuals who are dead. In the case of some BPDs there may be no indication whether the individuals referred to in the dataset are deceased or not. For example, the electoral roll will inevitably include individuals who are deceased, given that it is not continuously updated: such a dataset would require a warrant under the Act if it had been retained electronically for analysis by a Security and Intelligence Agency in the exercise of its statutory functions. If a BPD contains information about individuals who are known to be deceased, the relevant SIA may only decide to retain the dataset if it considers that it would be necessary and proportionate to do so for the purposes of its statutory functions.

Different statutory routes by which BPDs may be acquired

2.11 This code of practice applies not only to BPDs obtained under the information gateway provisions themselves (section 2(2)(a) of SSA and sections 2(2)(a) and 4(2)(a) of ISA), but also to BPDs where the mechanism for obtaining the datasets is subject to authorisation through the exercise of other statutory powers.

2.12 These other statutory powers include, but are not limited to, those exercisable under warrants issued under section 5 of ISA in respect of property interference otherwise than for the purpose of facilitating the obtaining of communications, equipment data or other

information; intrusive surveillance warrants issued under section 32 of the Regulation of Investigatory Powers Act 2000 ('RIPA'); directed surveillance authorisations issued under section 28 of RIPA; and covert human intelligence source authorisations issued under section 29 of RIPA. The application of this code of practice to BPDs obtained by exercise of the statutory powers listed above is without prejudice to any additional requirements specified in the legislation relevant to those statutory powers.

2.13 For the avoidance of doubt, this code of practice does not apply to BPD obtained by a Security and Intelligence Agency when it is exercising a power under a warrant or other authorisation issued or given under the Investigatory Powers Act [2016], for example, under a targeted or bulk interception or equipment interference warrant or under a bulk acquisition warrant (for bulk communications data). BPD acquired under such other Investigatory Powers Act powers will be subject to the applicable regime under the relevant part of the Act (see also paragraph 3.3 below). This is unless the Security and Intelligence Agency successfully applies to the Secretary of State to give a direction, with Judicial Commissioner approval, to disapply that regime in order to apply the BPD regime – see section 192 and paragraph 3.4 below. Once under the BPD regime, the provisions of this code of practice will apply.

3 BPD – general rules

Requirement for authorisation by warrant

3.1 The Act does not create any new power to obtain BPDs. Rather it requires that the retention and use of BPDs must be subject to an authorisation scheme and a comprehensive set of robust and transparent safeguards. Specifically, section 175 of the Act provides that a Security and Intelligence Agency may not exercise a power for the purpose of retaining or examining a BPD unless this is authorised by the issue of a warrant under Part 7 of the Act.

Types of warrant that may be issued

3.2 Section 175(3) describes the two types of warrant provided for by Part 7: a '**class BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, BPDs that fall within a class described in the warrant; and a '**specific BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, the particular BPD described in the warrant.

Exception to general requirement for authorisation by warrant

3.3 Section 176 explains the specific circumstances in which the general requirement under section 175 for a BPD warrant does not apply. Section 176(1) provides that the Part 7 authorisation scheme does not apply to BPD when this is obtained by a Security and Intelligence Agency by the exercise of **other** powers under the Act, for example, under a targeted or bulk interception or equipment interference warrant. An example of this might be where an email had been intercepted and a BPD was attached to the email. In such cases, the retention and examination of the BPD will be governed by the applicable regime under the relevant part of the Act – for example, the interception regime where a BPD is acquired as a result of interception.

3.4 However, under section 192, a Security and Intelligence Agency can apply to the Secretary of State for a direction that a BPD retained by it under a targeted or bulk interception or equipment interference warrant should have the provisions relating to that other power disapplied, and the BPD provisions of the Act applied instead. Such a direction can only be given with the approval of a Judicial Commissioner. Where an application for a direction under section 192 is made by the head of a Security and Intelligence Agency, consideration should also be given to whether an application for a specific warrant should be made at the same time. An application for a specific warrant should be made if the nature of the BPD which is subject to the direction is BPD that would require a specific warrant under Part 7. Under section 192(11), the Secretary of State may issue a specific warrant at the same time as giving a direction under this section. In issuing any direction, the Secretary of State is permitted to provide that any of the associated regulatory provisions which applied to the regime under which the BPD was obtained, should continue to apply once the direction has been issued (with or without modifications). In the case of a BPD obtained by interception which identifies itself as the product of interception, such a direction may not disapply the provisions in section 48 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act proceedings (see section 192(6)). Therefore, in making an application for a direction, a Security and Intelligence Agency

should consider which, if any, of the associated regulatory provisions it considers should – or should not – apply to the BPD, if the direction is issued.

3.5 Section 176(2) makes it clear that a BPD can be retained or examined to enable the information contained in it to be destroyed. This provision allows the Security and Intelligence Agencies to hold, temporarily, BPD which is no longer authorised by a warrant for the purpose only of ensuring that the relevant data is removed from their systems. If a warrant is cancelled or an application for a specific warrant is not approved, it will not always be possible for the Security and Intelligence Agency to delete the BPD immediately from its analytical systems. This is for two reasons. First, as the data has been ingested into wider analytical systems, it may take some time to delete the data – e.g. because the system must be taken off-line and/or because of the need for checks to ensure the correct data is deleted. Secondly, it may be that in some cases only part of a BPD is required to be deleted. This will, as a result, require examination of the dataset first to enable deletion.

3.6 Section 176(3) makes clear that other sections of Part 7 of the Act also provide for exceptions for the requirement to warrant in particular circumstances. These relate to a time limited period in which an Agency is conducting an initial examination of a potential BPD (section 190(5) – see paragraph 2.3 above and subsequent paragraphs) and for a limited period after the non-renewal or cancellation of a warrant (section 189(6) – see paragraph 5.47 and subsequent paragraphs).

4 BPD warrant applications

4.1 An application for a BPD warrant is made to the Secretary of State. The requirements set out in Part 7 of the Act only relate to the Security and Intelligence Agencies. An application for a BPD warrant therefore may only be made by or on behalf of the following persons:

- The Director General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).

4.2 All BPD warrants are issued by the Secretary of State. No BPD warrant may be issued unless and until it has been approved by a Judicial Commissioner (see paragraph 5.20 and subsequent paragraphs).

4.3 The only exception to this is a case where the Secretary of State considers that there is an urgent need to issue a specific warrant (see paragraph 5.24 and subsequent paragraphs). Even where the urgency procedure is followed, the Secretary of State still must personally authorise the warrant. In any case where the Secretary of State decides to issue a specific warrant (whether under the urgent procedure or otherwise), he or she must personally sign the warrant where reasonably practicable. However, a designated senior official can sign the warrant if it is not reasonably practicable for the Secretary of State to sign it. When a BPD warrant is issued, it is addressed to the person who submitted the application (or on whose behalf it was submitted).

4.4 Prior to submission, each application should be subject to a review within the Security and Intelligence Agency making the application. This involves consideration as to whether the application is for a purpose falling within sections 177(3)(a)(i) or 178(5)(a)(i) (in the interests of national security), 177(3)(a)(ii) or 178(5)(a)(ii) (for the purpose of preventing or detecting serious crime) or 177(3)(a)(iii) or 178(5)(a)(iii) (in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). The consideration of the application should also include whether the retention, or the retention and examination, of the BPD is both necessary and proportionate and whether the examination of the BPD is necessary for the operational purposes specified in the application (on which see paragraph 5.2 and subsequent paragraphs). There may be circumstances in which a Security and Intelligence Agency may consider it appropriate to apply for a warrant to retain a BPD before it has physically acquired that BPD.

Applications for class BPD warrants

4.5 Section 177 of the Act explains how the class BPD warrant authorisation process works. It specifies that an application for a class warrant must include:

- a description of the class of BPD to which the application relates; and
- if the Security and Intelligence Agency wishes to examine BPDs of that class, an explanation of the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine the BPDs falling within that class.
    - **Class BPD warrants**

4.6 Class BPD warrants are for those datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity, and the proportionality of using the data. This allows the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class: a class warrant might, for example, authorise a Security and Intelligence Agency to acquire travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.

4.7 Before submitting an application for a class warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:

- retention of BPDs within the class specified in the warrant is **necessary** for one or more of the purposes specified in sections 177 and 178 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- examination of BPDs within that class is **necessary** for one or more of the operational purposes to be specified in the class warrant and for one or more of the statutory purposes specified in sections 177 and 178 of the Act; and
- examining and retaining BPDs within that class in question is **proportionate** to the functions and purposes referred to in (a) and (b) above; only as much information will be obtained as is necessary to achieve those functions and purposes; and there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.

Applications for specific BPD warrants

4.8 Section 178 provides for two circumstances in which a Security and Intelligence Agency may apply to the Secretary of State for a specific BPD warrant. A specific warrant is a warrant for one specific BPD rather than a warrant for a class of BPDs. If either of these two circumstances apply, the relevant Security and Intelligence Agency should consider whether to make an application for a specific warrant.

4.9 In the '*Case 1*' scenario, the dataset does not fall within the scope of an existing class BPD warrant.

4.10 In the '*Case 2*' scenario, the dataset falls within a class of BPD authorised by an existing class warrant, but the relevant Security and Intelligence Agency nevertheless considers that it would be appropriate to seek a specific BPD warrant. Examples of the sort of situation where an Security and Intelligence Agency should seek a specific warrant are as follows:

- The nature or the provenance of the dataset raises particularly novel or contentious issues. An example of this could be when a Security and Intelligence Agency receives a BPD already covered by a class warrant, but the nature of the BPD is such that it could raise international relations concerns, and the Security and Intelligence Agency believes, in the light of this, that it would be appropriate for the Secretary of State to decide whether to authorise the retention and use of the particular BPD in question;
- The BPD has been assessed by the Security and Intelligence Agency as being relatively more intrusive because it contains a significant component of intrusive data (the degree of intrusiveness to be assessed in accordance with paragraph 4.11 and subsequent paragraphs); or

- The dataset contains a significant component of confidential information relating to members of sensitive professions. A 'sensitive profession' for these purposes includes lawyers, doctors, journalists, Members of Parliament and Ministers of religion. (References to a Member of Parliament include references to a Member of the UK Parliament, the Scottish Parliament, the Welsh Assembly, the Northern Ireland Assembly and a UK Member of the European Parliament.) (See paragraph 4.13 and subsequent paragraphs.)

Intrusiveness of data

4.11 When considering whether to retain and examine BPD, the Security and Intelligence Agencies will assess the degree or extent of the intrusiveness which retaining and examining the BPD would involve, that is to say the degree or extent of interference with individuals' right to privacy under Article 8 of the European Convention on Human Rights (ECHR). Each dataset is assessed on a case-by-case basis, and in the round, having regard (amongst other things) to the following factors or indicators:

- Is there an expectation of privacy? Did the individual provide their personal data in confidence to another organisation, not expecting that anyone except that organisation would have access to their data?
- Does the data consist of more than basic personal details (e.g. more than name, date of birth, address, telephone number and e-mail address)?
- Is there information on a person's activities or movements or travel?
- Does the data include 'sensitive personal data' within the meaning of section 2 of the Data Protection Act 1998 ("DPA" - see paragraph 11.8 of Annex A)?
- To what degree does the data, by virtue of its quality, nature or size, mean that, when it is examined, there will be a significant degree of intrusion into the privacy of individuals not of intelligence interest?

4.12 The indicators are not intended to be prescriptive; the presence of one or more will not necessarily result in the dataset as a whole being considered to be more intrusive. The indicators instead provide a framework which assists the relevant Security and Intelligence Agency in reaching a decision on the degree or extent of intrusiveness which retaining and examining the dataset would involve.

Confidential information relating to members of sensitive professions

4.13 Most BPDs do not include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to the sensitive professions. However, in the unlikely event that the Security and Intelligence Agency believed that a BPD dataset contained a significant component of confidential information relating to a member, or members, of a sensitive profession, the Agency must seek a specific warrant.

4.14 In this context, confidential information would include the content of communications between the professional, acting in their professional capacity, and another party, and any information which identified journalistic sources. Thus, for example, it would include the content of lawyer/client, doctor/patient and MP/constituent communications. However, information relating to a member of a sensitive profession is not, in and of itself, considered confidential. Confidential information in this context would not include the mere fact of membership of the profession, or basic biographical details of a member of the profession.

Thus, the fact that a solicitor's telephone number appeared in a telephone directory, would not be considered confidential information.

4.15 If required in an individual case, the Security and Intelligence Agency can seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner whether it would be appropriate for a specific BPD warrant to be sought. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

4.16 Section 178 specifies that an application for a specific BPD warrant must include:

- a description of the specific dataset to which the application relates; and
- an explanation of the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine the BPD.

4.17 Section 178(6) also enables a Security and Intelligence Service, when applying for a specific BPD warrant in respect of a particular BPD ('dataset A'), to request at the same time that the authorisation should extend to the retention and use of '**replacement datasets**', i.e. other bulk personal datasets that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

4.18 Before submitting an application for a specific warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:

- retention of the BPD is **necessary** for one or more of the statutory purposes specified in section 178 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- examination of the BPD is **necessary** for one or more of the operational purposes to be specified in the specific warrant and for one or more of the statutory purposes specified in section 178 of the Act; and
- examining and retaining the BPD in question is **proportionate** to what is sought to be achieved by the conduct.

5 Authorisation and approval of warrants

Authorisation of class and specific BPD warrants by a Secretary of State

5.1 The Secretary of State may only issue a warrant under sections 177 (class BPD warrants) or 178 (specific BPD warrants) if the Secretary of State considers the following tests are met:

- The warrant is necessary:[1]
  - In the interests of national security;
  - For the purpose of preventing or detecting serious crime; or
  - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.
- The conduct authorised by the warrant is proportionate to what it seeks to achieve.
- Each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 177(3)(a) or section 178(5)(a). (See paragraph 5.2 and subsequent paragraphs for more on operational purposes.)
- There are satisfactory safeguards in place. The Secretary of State must consider that satisfactory arrangements are made for storing the BPD and for protecting them from unauthorised disclosure. (See paragraph 7.3 and subsequent paragraphs).
- A Judicial Commissioner has approved the issue of the warrant. Except in the case of an urgent specific warrant, the Secretary of State may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner (see paragraph 5.20 and subsequent paragraphs).

What are operational purposes?

5.2 Section 191 provides specific safeguards relating to the selection of data contained in a BPD under a class or specific BPD warrant for examination. References to examination of data from a BPD are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant (see section 225 of the Act for general definitions in the Act).

5.3 Sections 191(1) and 191(2) make clear that selection for examination, of data from a BPD, may only take place for one or more of the operational purposes that are specified on the warrant. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to select for examination, data from a BPD, otherwise than in accordance with a specified operational purpose. For the avoidance of doubt, data from a BPD selected for an operational purpose can, where it is necessary and proportionate to do so, be used, disclosed and retained for any statutory purpose.

[1] A single warrant can be justified on more than one of the grounds listed.

5.4 Sections 177 and 178 make clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, section 183(5) specifies that it is not sufficient under the Act for operational purposes simply to use the wording of one of the statutory purposes. Whilst the purposes may still be general ones, they must include more detail that a statutory purpose to ensure that the BPD can only be selected for examination for specific reasons. Operational purposes provide the Secretary of State and the Judicial Commissioner with a more granular understanding of the purposes for which the BPD will be retained and examined.

5.5 The Security and Intelligence Agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a BPD warrant needs to reflect this. New operational purposes will therefore be required over time. The Act provides (under section 186) that a BPD warrant may be modified to amend the operational purposes specified on it; for further detail on the process for this, see later sections of this chapter.

5.6 In line with this, the Security and Intelligence Agencies will need to ensure the full range of their BPD warrants are relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. They will need to identify operational purposes that need to be added to or removed from BPD warrants, including in urgent circumstances. This would be done through the modifications process set out in the Act.

5.7 Some operational purposes that may need to be specified on a bulk warrant will be consistent across the three Agencies, although some purposes will be relevant to a particular Agency or two of the three. Operational purposes should as far as possible be consistent across the bulk capabilities provided for by the Act.

5.8 The Act does not limit the number of operational purposes that may be specified in the warrant. Where the necessity and proportionality test is satisfied, a warrant may include all operational purposes currently in use by an Agency. BPDs are likely to have potential relevance and utility across the full range, or most, of a Security and Intelligence Agency's operations or investigations. In the majority of cases, it will therefore be highly likely that it would be considered necessary for BPD warrants to specify the full range of an Agency's operational purposes.

5.9 An example of an "operational purpose" in the context of the security and intelligence agencies' international counter-terrorism work might be 'The Investigation, assessment and disruption of attack planning by Daesh in Iraq/Syria against the UK.'

Necessity and proportionality

5.10 Where the retention or examination of BPD involves an interference with an individual's rights under Article 8 (right to respect for private and family life) of the ECHR, this will only be justifiable if the interference is necessary and proportionate. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the statutory purposes set out in section 177(3) and 178(5) of the Act:

- In the interests of national security;
- For the purpose of preventing or detecting serious crime;
- In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

5.11 The Secretary of State must also believe that the retaining or examination of the BPD is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into privacy against the need for the activity in investigative, operational or capability terms.

When will retaining or examining BPD be necessary?

5.12 What is necessary in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the 'necessity' requirement in relation to retention and examination, the Security and Intelligence Agencies and the Secretary of State must consider why retaining or retaining and examining the bulk personal dataset is 'really needed' for the statutory and operational purposes referred to in paragraph 5.1 above.

5.13 Chapter 7 includes further material on the necessity considerations that apply to examination of BPDs.

When will retaining or examining BPD be proportionate?

5.14 The retention or examination of the bulk personal dataset must also be proportionate to what is sought to be achieved by the conduct authorised under the warrant. In order to meet the 'proportionality' requirement, the Security and Intelligence Agencies and the Secretary of State must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the dataset and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the dataset.

5.15 The Security and Intelligence Agency and the Secretary of State must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the dataset and the importance of the operational purposes to be achieved. The Security and Intelligence Agency and the Secretary of State must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.

5.16 The warrant will not be proportionate if it is excessive in the overall circumstances of the case. The conduct authorised should bring an expected benefit to the Security and Intelligence Agency's investigations or operations and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not necessarily render intrusive conduct proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

5.17 Chapter 7 includes further material on the proportionality considerations that apply to examination of BPDs.

Authorisation of a specific warrant: senior officials

5.18 The Act permits that when it is not reasonably practicable for the Secretary of State to sign a specific BPD warrant a senior official may sign the warrant on their behalf. Typically this scenario will arise where the appropriate Secretary of State is not physically available to sign the warrant because, for example, he or she is on an external visit or in their constituency. The Secretary of State must still personally authorise the BPD warrant. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant the warrant must not be issued. When a warrant is issued in this way the warrant instrument must contain a

statement to that effect. A warrant that has been signed by a senior official is not an urgent warrant unless there is a statement to that effect from the Secretary of State. Except in urgent cases the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

5.19 The Act does not mandate how the Judicial Commissioner must show or record his or her decision. These practical arrangements should be agreed between the relevant Government Departments and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. It is important that a written record is taken of any such approvals.

Approval of the issue of BPD warrants by a Judicial Commissioner

5.20 Before a class or specific BPD warrant can be issued by the Secretary of State, it must be approved by a Judicial Commissioner.

5.21 Section 179 of the Act provides that, when deciding whether to approve the decision to issue a BPD warrant, the Judicial Commissioner must review the Secretary of State's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. The Judicial Commissioner must also review the Secretary of State's conclusions as to whether each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary, and whether the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 177(3)(a) or section 178(5)(a). In reviewing these matters, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations.

5.22 If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

- not issue the warrant;
- refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).

5.23 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant. There is no avenue of appeal available to the Secretary of State.

Urgent authorisations

5.24 The Act makes provision (see sections 180 – 182) for cases in which a specific BPD warrant is required urgently. It is not possible to seek an urgent class BPD warrant.

5.25 In addition to the tests sets out at paragraph 5.1 above, the Secretary of State must believe that there was an urgent need to issue the warrant. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. Accordingly, urgent warrants can be issued by the Secretary of State without prior approval from a Judicial Commissioner. The requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should, therefore, fall into at least one of the following three categories:

- Imminent threat to life or serious harm – for example, an individual has been kidnapped and it is assessed that his life is in imminent danger;
- A significant intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas.
- A significant investigative opportunity – for example, there is an imminent attempt to smuggle weapons into the UK to a known terrorist by boat; we may wish to use BPD to identify the vessel to prevent the weapons reaching the terrorist.

5.26 The decision by the Secretary of State to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue. In the case of warrants signed by a senior official, the Judicial Commissioner's review should be on the base of a written record, including any contemporaneous notes, of the oral briefing of the Secretary of State by a senior official (and any questioning or points raised by the Secretary of State).

5.27 If the Judicial Commissioner retrospectively agrees to the Secretary of State's issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent BPD warrants.

5.28 The Judicial Commissioner may refuse to approve the Secretary of State's decision to issue the urgent warrant. If that is the case, the urgent warrant ceases to have effect and may not be renewed. However, the Judicial Commissioner may:

- direct that any BPD retained in reliance on the warrant must be destroyed; or
- impose conditions as to the use or retention of any such datasets. The Security and Intelligence Agency or the Secretary of State can make, or be required to make by the Judicial Commissioner, representations to the Commissioner about requirements to destroy datasets and/or conditions relating to use or retention.

5.29 If the Judicial Commissioner does not approve the urgent warrant, the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant stopped as soon as possible. In such a scenario, activity undertaken by virtue of that urgent warrant remains lawful, including activity in process at the time the warrant ceases to have effect which it is not reasonably practicable to stop.

5.30 A flowchart setting out the urgent authorisation process is provided at Annex B.

Duration of BPD warrants

5.31 Section 184 provides that, for non-urgent warrants, the warrant comes into effect at the point at which it is issued or, in the case of a renewed warrant, the day following the day on which it would otherwise have ceased to have effect. In either case, the warrant lasts for six months. An urgent warrant lasts for five working days after the day on which it was issued.

5.32 Where modifications to a BPD warrant are made, the warrant expiry date remains unchanged.

5.33 Where a change in circumstance leads the Security and Intelligence Agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the Agency

must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

Modification of a BPD warrant

5.34 Section 186 provides for modifications of BPD warrants. There are two kinds of modifications: (a) major modifications, which **add** or **vary** any operational purpose specified in the BPD warrant; and (b) minor modifications, which **remove** any operational purpose specified in the warrant. A class or specific BPD warrant may be modified by an instrument under the provisions at section 186.

5.35 A modification to add or vary an operational purpose must be made by the Secretary of State and, except where the Secretary of State considers it urgent, the decision to make the modification must be approved by a Judicial Commissioner before the modification comes into force. (See paragraph 5.38 and subsequent paragraphs for more on urgent modifications.) A modification to remove an operational purpose may be made by Secretary of State or a designated senior official acting on behalf of the Secretary of State.

5.36 If a modification removing an operational purpose is made by a designated senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. This can be done in writing or orally, though if it is done orally a record must be kept (see Chapter 8 of this Code for further information on record-keeping). It should happen as quickly as reasonably practicable. If at any time the Secretary of State, or a senior official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they must modify the warrant to remove that operational purpose.

5.37 The modification instrument should be addressed to the person to whom the warrant was issued (i.e. the head of the relevant Security and Intelligence Agency).

Urgent modification of a BPD warrant

5.38 Sections 186 and 187 also provide for urgent modifications of BPD warrants. An operational purpose may be added to or varied on an urgent basis. In such a case, the Secretary of State's decision to make the modification does not need to be approved by a Judicial Commissioner prior to having effect. A senior official acting on behalf of the Secretary of State may make the modification with the express authorisation of the Secretary of State. A Judicial Commissioner must decide whether to approve the decision to make such a modification within five working days.

5.39 If the Judicial Commissioner does not approve the urgent modification, the warrant has effect as if the modification had not been made, and the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant by virtue of that modification is stopped as soon as possible. In such a scenario, activity undertaken by virtue of that modification remains lawful, including activity in process at the time the modification ceases to have effect which it is not reasonably practicable to stop.

Renewal of BPD warrants

5.40 The Secretary of State may renew a warrant at any point before its expiry date (section 185 of the Act). Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.1 above. In particular, the applicant must give an assessment of the value derived to date from the specific BPD or from the class of BPD

in question, and explain why it is continues to be necessary to retain and/or examine the specific BPD(s) or the class of BPD, and why this continues to be proportionate.

5.41 In deciding whether to renew a BPD warrant, the Secretary of State must also consider whether the examination of the specific BPD or the class of BPD continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes (as set out in the first bullet-point in paragraph 5.1 above) on the warrant.

5.42 Where the Secretary of State is satisfied that the retention and/or examination of the BPD continues to meet the requirements of the Act, the Secretary of State may renew the warrant. In all cases, a BPD warrant may only be renewed if the decision to renew that warrant has been approved by a Judicial Commissioner. The renewed warrant is valid for six months from the day following the day on which it would otherwise have ceased to have effect.

5.43 A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Cancellation of warrant

5.44 The Secretary of State, or a senior official acting on his or her behalf, may cancel a BPD warrant at any time (see section 188). Such persons must cancel a BPD warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on the grounds of any one of the statutory purposes for which it was issued. The Security and Intelligence Agencies will therefore need to keep their BPD warrants under continuous review and must notify the Secretary of State if they assess that a warrant is no longer necessary. In practice, the responsibility to cancel a warrant will normally be exercised by a senior official in the warrant granting department on behalf of the Secretary of State.

5.45 The cancellation instrument will be addressed to the person to whom the warrant was issued.

5.46 The cancellation of a warrant does not prevent the Secretary of State deciding, with Judicial Commissioner approval, to issue a new warrant, covering the same or different bulk personal datasets and operational purposes, in the future should it be considered necessary and proportionate to do so. Where there is a requirement to modify the warrant, other than to amend the operational purposes for which the data can be examined, then the warrant may be cancelled and a new warrant issued in its place.

Non-renewal or cancellation of class BPD warrants

5.47 Section 189 provides for the situation where a BPD warrant is not renewed or is cancelled and, in particular, sets out the process for dealing with the material that was retained under the warrant in question. The material may be destroyed; section 189(2) ensures retention or examination of the material for the purpose of deleting the material is lawful. But depending on the reasons why the warrant has been cancelled or not renewed, the relevant Security and Intelligence Agency may consider it necessary and proportionate to retain some or all of the material that had been retained under the authority of that warrant. Section 189 therefore includes bridging provisions to ensure any retention and examination of the material in question is lawful pending any authorisation via a new warrant. The relevant Security and Intelligence Agency may apply for a new class or specific BPD warrant within five working days (section 189(2)).

5.48 If the relevant Agency needs further time to consider whether to apply for a new warrant, it may instead apply to the Secretary of State for authorisation to retain or retain and examine some or all the material retained under the warrant. The Agency can only apply for such authorisation if it is considering whether to apply for a new class or specific BPD warrant to authorise retention or retention and examination of the material. In particular, under section 189(6) and 189(7), the Agency has five working days in which to decide whether it wants to apply for such authorisation. Retention and examination of that data is lawful pending the Secretary of State's decision under such an application. If the agency so applies, the Secretary of State can then direct that any of the material should be destroyed or, with the approval of the Judicial Commissioner, can authorise the retention or examination of any of the material, subject to such conditions as the Secretary of State considers appropriate. Retention or examination is lawful under such a direction. During that period, the agency must consider whether to and then apply for a new warrant as soon as reasonably practicable and in any event within three months. Retention and examination remains lawful for the period between the agency applying for a new warrant and the determination of that application, even if determination takes place after the end of the three month period.

5.49 These provisions may be required if, for example, the Secretary of State is no longer satisfied that all the individual bulk personal datasets in a BPD class authorised by a warrant should be retained, because e.g. the class is considered too wide in scope, but would be willing to issue to the relevant Security and Intelligence Agency a class BPD warrant for a more restricted class of BPD (or a specific warrant). In such a situation, the Secretary of State might be satisfied that it was necessary and proportionate for the relevant Intelligence Service to retain some of the individual bulk personal datasets in the BPD class or a subset or subsets of that material, pending the issue of a new class warrant or specific warrant. Or the Secretary of State may be willing to authorise the continued retention and examination of some but not all the material held under a specific BPD warrant.

5.50 If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, section 189(4) requires that he or she must give the Secretary of State written reasons for this. If it was a Judicial Commissioner other than the Investigatory Powers Commissioner who did not approve the decision, the Secretary of State can ask the Investigatory Powers Commissioner to decide whether to approve the decision (section 189(5)).

6 Authorisation of the retention and use of BPDs falling within a class BPD warrant

6.1 For the purpose of dealing with BPD falling within the scope of an existing class BPD warrant, each Security and Intelligence Agency should have a formal internal authorisation procedure which must be complied with.

6.2 Before deciding to retain a BPD falling within the scope of an existing class BPD warrant ("the relevant class warrant") for the purpose of the exercise of its statutory functions, the Security and Intelligence Agency must be satisfied that:

- the BPD in question falls within the scope of the relevant class warrant;
- retention of the BPD is **necessary** for one or more of the relevant Agency's statutory functions;
- each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 177(3)(a) or section 178(5)(a)
- retaining and examining the BPD in question is **proportionate** to what is sought to be achieved by the conduct;
- only as much information will be obtained as is **necessary** to achieve those functions and purposes; and
- there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.

6.3 An explanation of the necessity and proportionality tests is provided at paragraph 5.10 and subsequent paragraphs and of operational purposes at paragraph 5.2 and subsequent paragraphs.

6.4 Before a new dataset falling within the scope of a class BPD warrant is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions, the relevant staff in that Agency should consider the factors set out in paragraph 6.2 above and complete the formal internal authorisation procedure. The authorisation procedure involves an application to a senior manager which should include the following:

- a description of the particular BPD, including details of the personal data contained in the dataset, and any confidential information relating to members of sensitive professions or data that is considered to be intrusive (as assessed by reference to the factors in paragraph 4.11 and subsequent paragraphs) of which staff are aware;
- a description of the class BPD warrant within which the dataset falls;
- the justification for retention and examination, including the operational purposes for which examination of the dataset is required, the statutory functions which are engaged and the necessity and proportionality of the proposed retention and examination;
- an assessment of the level of intrusion into privacy;
- the consideration and advice of the relevant Agency's legal advisers; and

- the extent of political, reputational or other risk.

6.5 The relevant Security and Intelligence Agency should consult line or senior management for guidance. They may also seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant warrant-issuing Department), the Secretary of State and/or the Investigatory Powers Commissioner. If the Security and Intelligence Agency is not clear on whether an internal authorisation is appropriate, then they should seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

6.6 Once authorised, the completed application should be stored on a record by the appropriate Security and Intelligence Agency's information governance/compliance team, which will include the date of approval. This record should also contain the date when the Agency decided to retain the dataset after the initial examination referred to in paragraph 2.3 and subsequent paragraphs, which should be the date used for the review process (for which see paragraph 7.18 and subsequent paragraphs).

7 Safeguards

7.1 This section sets out the safeguards which each Security and Intelligence Agency should put in place in relation to storage of bulk personal datasets (whether acquired under class BPD or specific BPD warrants), record-keeping, access to and examination of BPDs, disclosure and review and retention of BPDs. The Secretary of State may only issue a BPD warrant if s/he considers that arrangements made by the relevant Security and Intelligence Agency for storing BPD and for protecting the datasets from unauthorised disclosure are satisfactory (as set out in sections 177(3)(d) and 178(5)(d)).

7.2 The safeguards in this chapter are in addition to those set out in earlier chapters of this code, including the requirement for the retention and examination of BPD to be necessary and proportionate for it to take place; the need to ensure only as much information will be obtained as is necessary and that there is no reasonable alternative that will still meet the proposed objective in a less intrusive way; the particular considerations that need to be given to the intrusiveness of the data and the extent to which that data includes confidential information relating to sensitive professions; and the requirement for Secretary of State and Judicial Commissioner approval for BPD warrants. (See chapters 4 and 5).

Storage

7.3 Each Security and Intelligence Agency should maintain robust data security and protective security standards. They should have in place handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is effectively 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 it is detected and that appropriate disciplinary action is taken. In particular, each Agency should 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; and
- A security-vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Safeguards before BPD is made accessible

7.4 Where BPD contains a significant component either of intrusive data (see paragraph 4.11 and subsequent paragraphs) or of confidential information relating to sensitive professions, before such BPD is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions the relevant Agency should consider whether access by its staff to such data should be subject to any particular restrictions, including sensitive fields being suppressed or deleted, or additional justification required to access and examine sensitive data-fields.

Access and examination

7.5 In relation to information held in bulk personal datasets, each Security and Intelligence Agency should have in place the following additional measures:

- Access to and examination of the information contained within the bulk personal datasets should be strictly limited to those with an appropriate business requirement to use these data;
- Individuals may only access information within a bulk personal dataset if examination of the BPD is necessary for one or more of the operational purposes specified in the relevant class warrant or specific warrant and for one or more of the relevant statutory purposes specified in the Act (see paragraph 5.10 and subsequent paragraphs);
- If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, (in addition to satisfying the condition in the above bullet) they may only access and examine 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 set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
- Before accessing or disclosing information, individuals must also consider whether to do so would be proportionate (as described in paragraph 5.10 and subsequent paragraphs and below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;
- Users should receive mandatory training regarding their professional and legal responsibilities, including the application of the provisions of the Act and this Code of Practice. Refresher training and/or updated guidance should be provided when systems or policies are updated;
- Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal data by staff in order to detect misuse or identify activity that may give rise to security concerns;
- Appropriate disciplinary action should be taken in the event of inappropriate behaviour being identified;
- Users should be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution; and
- The Secretary of State must ensure that the safeguards are in force before any BPD warrant authorising use can begin.

7.6 The Security and Intelligence Agencies should also take the following measures – by establishing the necessary underpinning working practices - to reduce the level of interference with privacy arising from the retention and examination of bulk personal datasets:

- Minimising the number of results which are presented for analysis, by training and requiring staff to frame queries in a proportionate way; and
- If necessary, confining access to specific datasets (or subsets thereof) to a limited number of analysts.

Personnel security

7.7 All persons within the Security and Intelligence Agencies who may have access to BPDs or need to see any reporting in relation to them must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one Agency to disclose BPDs to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

Additional access safeguards for confidential information relating to sensitive professions

7.8 The Security and Intelligence Agencies should ensure that, before SIA staff who are searching a bulk personal dataset specifically target for access or examination confidential information relating to members of sensitive professions, **special consideration** is given to the necessity and proportionality justification for the interference with privacy that will be involved.

7.9 The Security and Intelligence Agencies should also ensure that particular care is taken when deciding whether to seek such access to data or information of the kind described in paragraph 7.8 above, and should consider whether there might be unintended consequences of such access and whether the public interest is best served by this, and only to do so if authorised beforehand by a senior manager.

7.10 In all cases where SIA staff intentionally seek to examine such data or information, they should be required to record the fact that such information or data has been accessed and selected and flag this to the Investigatory Powers Commissioner at the next inspection. Likewise, where SIA staff are aware that in searching a bulk personal dataset they have unintentionally accessed such data or information but have decided to select and retain it, they should be required to record the fact of this access and intentional selection and flag this to the Investigatory Powers Commissioner at the next inspection.

Disclosure

7.11 Information in bulk personal datasets held by a Security and Intelligence Agency (whether acquired under class BPD or specific BPD warrants) may only be disclosed to persons outside the relevant Agency if the following conditions are met:

- that the objective of the disclosure falls within the Agency's statutory functions or is for the additional limited purposes set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective; and
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

7.12 In order to meet the 'necessity' requirement in relation to disclosure, the Security and Intelligence Agency must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Agency or for the additional limited purposes set out in the information gateway provisions.

7.13 The disclosure of the bulk personal dataset must also be proportionate to the purpose in question. In order to meet the 'proportionality' requirement, the relevant Security and Intelligence Agency 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 Agency's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. The relevant Security and Intelligence Agency 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.

7.14 Before disclosing any bulk personal data, the relevant Security and Intelligence Agency must either take reasonable steps to ensure that the intended recipient organisation has, and will maintain, satisfactory arrangements regarding the use of the BPD, and for safeguarding the confidentiality of the data and ensuring that it is securely handled. What steps should to be viewed as reasonable in any particular instance of disclosure will depend on the circumstances of the case, but will include consideration of the nature of the disclosure and what is known about the recipient.

7.15 Where the BPD has been acquired under an interception warrant, the relevant Security and Intelligence Agency must also consider whether the restrictions on the use of disclosure of material obtained under an interception warrant into legal proceedings, will be relevant (see section 192(6)).

7.16 These conditions for disclosure apply equally to the disclosure of an entire bulk personal dataset, a subset of the dataset, or an individual piece of data from the dataset. Disclosure of the whole (or a subset) of a bulk personal dataset is subject to internal authorisation procedures in addition to those that apply to an individual item of data. The authorisation process requires an application to a senior manager designated for the purpose which is required to set out the following:

- a description of the dataset it is proposed to disclose (in whole or in part), including details of the personal data contained in the dataset, and any significant component of intrusive data or confidential information relating to sensitive professions of which staff are aware;
- the operational and legal justification for the proposed disclosure, and the necessity and proportionality of the disclosure;
- an assessment of the level of intrusion into privacy;
- the extent of political, reputational or other risk;
- whether any caveats or restrictions should be applied to the proposed disclosure; and
- confirmation that reasonable steps have been taken to ensure that disclosure to the recipient organisation is in accordance with paragraph 7.14 above.

7.17 This information should be included, so that the senior manager can then consider the factors in paragraph 7.11 with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant Department), the Secretary of State and/or the Investigatory Powers Commissioner.

Review of retention and deletion

7.18 Each Security and Intelligence Agency must regularly review the operational and legal justification for its **continued retention, examination and use** of each bulk personal dataset retained by it under a class warrant. The frequency of the review – as agreed with the Secretary of State – should be guided by the level of intrusion which is generated by the

holding of the BPD (and any other factors that the Security and Intelligence Agency or the Secretary of State consider appropriate), and must in any event be such as to ensure that the justification for the continued retention of bulk personal datasets covered by the relevant class warrant is adequately considered.

7.19 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 of the dataset and its examination for the operational purposes, with examples of use;
- The extent to which the dataset originally acquired needs to be replaced by a more up-to-date;
- The level of intrusion into privacy;
- The extent of political, reputational or other risk; and
- Whether any caveats or restrictions should be applied to continued retention.

Destruction

7.20 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 Security and Intelligence Agency should be destroyed. Section 225 of the Act provides definition of 'destroy'. Each Agency should report to the Secretary of State, on a six-monthly basis, with a list of all BPD destroyed in the previous six months.

Other management controls

7.21 The retention and disclosure of a bulk personal dataset should be subject to scrutiny in each Security and Intelligence Agency, which should put in place an effective system to ensure each of the following:

- that each bulk personal dataset has been properly obtained;
- that access to BPD is permitted only for the specified operational purposes and for the relevant SIA's statutory functions;
- that any disclosure is properly justified; and
- that retention and examination of the BPD remains necessary for the specified operational purposes and the proper discharge of the relevant SIA's statutory functions and is proportionate to achieving that objective.

7.22 Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal datasets by staff in order to detect misuse or identify activity that may give rise to security concerns.

7.23 Any such identified activity initiates a formal investigation process in which legal, policy and 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.

7.24 All reports on audit investigations are required to be made available to the Investigatory Powers Commissioner for scrutiny (see chapter 9 below).

8 Record-keeping and error-reporting

8.1 The oversight regime allows the Investigatory Powers Commissioner to inspect the warrant application upon which the authorisation was based, and the applicant may be required to justify the content. Each Security and Intelligence Agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for BPD warrants and all applications made for the renewal of such warrants;
- All BPD warrant instruments, associated schedules, renewal instruments and copies of modification applications; and
- Where any application is refused, the grounds for refusal as given by the Secretary of State.

8.2 Records should also be kept by the relevant Department of State of the warrant authorisation process. This will include:

- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the BPD warrant;
- Written records, including contemporaneous notes, of requests for urgent authorisations of warrants or modifications; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice / applications to the Investigatory Powers Commissioner if there is an appeal.

8.3 Each Security and Intelligence Agency must also keep a record of the following information to assist the Investigatory Powers Commissioner to carry out his/her statutory functions:

- The number of applications for (a) class and (b) specific BPD warrants submitted.
- The number of applications for (a) class and (b) specific BPD warrants refused by the Secretary of State.
- The number of decisions to issue (a) class and (b) specific BPD warrants refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse the Secretary of State decision to issue (a) class and (b) specific BPD warrants.
- The number of (a) class and (b) specific BPD warrants issued by the Secretary of State and approved by a Judicial Commissioner.
- The number of times an urgent specific BPD warrant has been (a) submitted and (b) authorised by the Secretary of State and issued by a senior official.
- The number of times that the decision to authorise an urgent specific BPD warrant has subsequently been refused by a Judicial Commissioner.
- The number of renewals of (a) class and (b) specific BPD warrants that were made.
- The number of (a) class and (b) specific BPD warrants that were cancelled.

- The number of (a) class and (b) specific BPD warrants extant at the end of the calendar year.
- The number and details of modifications to add an operational purpose to the warrant, vary an operational purpose or remove an operational purpose from the warrant.
- The number and details of urgent modifications to add an operational purpose to the warrant or vary an operational purpose the warrant.
- The number and details of urgent modifications to add or vary an operational purpose (including on an urgent basis) where the decision was refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve a decision to modify an urgent specific BPD warrant.
- A record of BPDs held that fall within a particular class warrant (see chapter 6 above)
- A record of any intentional examination of confidential information relating to sensitive professions (see paragraph 7.8 and subsequent paragraphs)
- A list of all BPD deleted or destroyed in the previous six months (see paragraph 7.20)

8.4 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by the Commissioner. Guidance on record keeping may be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by the Security and Intelligence Agencies.

8.5 The Investigatory Powers Commissioner will use this information to inform their oversight and, where appropriate, include in their report to the Prime Minister about the carrying-out of the functions of the Judicial Commissioners. The Prime Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of the report if, in the opinion of the Prime Minister, the publication would be contrary to the public interest or prejudicial to national security, prevention or detection of serious crime, or the continued discharge of the functions of the overseen public authorities.

8.6 Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management. And any serious breaches of safeguards that have resulted in an unauthorised or unjustifiable interference with privacy, as agreed with the Investigatory Powers Commissioner, must be reported to the Commissioner. The Investigatory Powers Commissioner may issue guidance in respect of error-reporting which the Security and Intelligence Agency must have regard to.

9 Oversight

9.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the IPC'), whose remit includes providing comprehensive oversight of the retention, use or disclosure of bulk personal datasets by the security and intelligence agencies and adherence to the practices and processes described by this code. By statute the IPC will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The IPC will be supported by inspectors and others, such as technical experts, qualified to assist the IPC in their work.

9.2 The IPC, and those that work under the authority of the Commissioner, will ensure compliance with the law and this code by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister.

9.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out a full and thorough inspection regime. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the IPC and anyone who is acting on behalf of the Commissioner.

9.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in error reporting provisions of chapter 8 of the code, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

9.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 8 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

9.6 The Commissioner must also inform the affected individual of their right to apply to the IPT (see chapter 10 for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate. The IPC must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions for reasons of national security. Only the Prime Minister will be able to authorise redactions to the IPC's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

9.7 The IPC may also report, at any time, on any of its investigations and findings as they see fit. These reports will also be made publically available subject to national security considerations. Public authorities and communications service providers may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible this guidance will be published in the interests of public transparency.

9.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

10 Complaints

10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

10.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: http://www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

10.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

11 Annex A

The Security Service Act 1989 and the Intelligence Services Act 1994

11.1 The **Security Service Act 1989** (SSA) provides that the functions of the Security Service are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime.

11.2 The **Intelligence Services Act 1994** (ISA) sets out the functions of the Secret Intelligence Service (SIS) and Government Communications headquarters (GCHQ). In the case of SIS these are: obtaining and providing information relating to the actions or intentions of persons outside the British Islands; and performing other tasks relating to the actions or intentions of such persons. In the case of GCHQ these are: monitoring, making use of or interfering with communications and related equipment; and providing advice on information security and languages. ISA goes on to provide that their respective functions (with the exception of GCHQ's information security and language functions) may only be exercisable (a) in the interests of national security, with particular reference to the defence and foreign policies of the UK Government, (b) in the interests of the economic well-being of the UK, or (c) in support of the prevention or detection of serious crime.

11.3 The information gateway provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of ISA 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 (ii) that no information is disclosed except so far as is necessary for those functions and purposes or for the additional limited purposes set out in section 2(2)(a) of ISA (in the interests of national security, for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings), section 4(2)(a) of ISA (for the purpose of any criminal proceedings) and section 2(2)(a) of SSA (for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).

11.4 SSA and ISA accordingly impose specific statutory limits on the information that each of the Security and Intelligence Agencies can obtain, and on the information that each can disclose. These statutory limits do not simply apply to the obtaining and disclosing of information from or to other persons in the United Kingdom: they apply equally to obtaining and disclosing information from or to persons abroad.

The Counter-Terrorism Act 2008

11.5 Section 19 of the **Counter-Terrorism Act 2008** confirms that ‘any person’ may disclose information to the Agencies for the exercise of their respective functions, and disapplies any duty of confidence (or any other restriction, however imposed) which might otherwise prevent this. It further confirms that information obtained by any of the Security and Intelligence Agencies 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. For example, information that is obtained by the Security Service for national security purposes can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime.

The Human Rights Act 1998

11.6 Each of the Security and Intelligence Agencies is a public authority for the purposes of the Human Rights Act 1998. When obtaining, using, retaining and disclosing bulk personal datasets, the Security and Intelligence Agencies must therefore (among other things) ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. In practice, this means that any interference with privacy must be both necessary for the performance of a statutory function of the relevant Intelligence Service and proportionate to the achievement of that objective.

The Data Protection Act 1998

11.7 Section 1(1) of the **Data Protection Act 1998** defines '*personal data*' as:

"data which relate to a living 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. in this case, the relevant Intelligence Service], 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".

11.8 Section 2 of the DPA defines "sensitive personal data" as meaning personal data in relation to a data subject consisting of information as to 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
- 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.

11.9 Each of the Security and Intelligence Agencies is a data controller in relation to all the personal data that it holds. Accordingly, when the Security and Intelligence Agencies use any bulk data that contain personal data, they must ensure that they comply with the Data Protection Act 1998 (except in cases where exemption under section 28 is required for the purpose of safeguarding national security).

12 Annex B


If the Secretary of State agrees the requirement for a warrant is urgent (and necessary and proportionate) then the warrant may be issued immediately. This urgent warrant must be reviewed by a Judicial Commissioner within three working days. The Investigatory Powers Commissioner must be notified that the urgent warrant has been issued and will have three working days to apply Judicial Review principles to the Secretary of State's decision.
The warrant is cancelled before the Judicial Commissioner has considered the warrant. The Judicial Commissioner will retrospectively consider the application. If they do not approve the warrant, they may then determine what happens to any material already obtained under the warrant.
The Judicial Commissioner approves the decision to issue the warrant then it may continue for five working days.
The Judicial Commissioner does not approve the decision to approve the warrant: all activity must cease. The Judicial Commissioner may determine what happens to any material already obtained under the warrant.
After three days if the warrant remains necessary the warrant requesting agency can seek to renew it. If the Secretary of State agrees that the warrant is both necessary and proportionate then the warrant will be passed to a Judicial Commissioner to review on judicial review principles
The Judicial Commissioner approves the decision to issue the renewal and it lasts for six months.
The Judicial Commissioner does not approve the decision, the warrant will not be renewed and all activity will cease.
The Secretary of State may ask the Investigatory Powers Commissioner to review the Judicial Commissioner's decision.
The Investigatory Powers Commissioner also refuses to approve the decision and the warrant cannot be renewed.
The Investigatory Powers Commissioner overturns the original decision and approves the decision. The warrant can be issued and lasts for six months.