Home Office

Intelligence Services' Retention and Use of Bulk Personal Datasets

DRAFT Code of Practice

December 2017

Intelligence Services' Retention and Use of Bulk Personal Datasets

DRAFT Code of Practice

Presented to Parliament pursuant to paragraph 4(5) of Schedule 7 to the Investigatory Powers Act 2016

December 2017

This publication is available at: www.gov.uk/government/publications.

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk.

Contents

1 Introduction 3
2 Scope and definitions 4
Different statutory routes by which BPDs may be acquired 6
3 BPDs – general rules 7
Requirement for authorisation by warrant 7
Types of warrant that may be issued 7
Exception to general requirement for authorisation by warrant 7
4 BPD warrant applications 10
Class BPD warrants 11
Applications for class BPD warrants 11
Restriction on use of class BPD warrants 12
Confidential information relating to members of sensitive professions. 12
Applications for specific BPD warrants 14
BPDs containing 'protected data' – further restriction on class warrants and provision for attaching conditions to specific warrants 16
5 Authorisation of class and specific BPD warrants by a Secretary of State 23
What are operational purposes? 24
Necessity and proportionality 26
When will retaining or examining a BPD be necessary? 27
When will retaining or examining a BPD be proportionate? 27
Authorisation of a specific warrant: senior officials 28
Judicial Commissioner Approval 28
Urgent authorisations 29
Duration of BPD warrants 31
Modification of a BPD warrant 31
Urgent modification of a BPD warrant 32
Renewal of BPD warrants 32
Cancellation of warrants 34
Non-renewal or cancellation of class BPD warrants 34
6 Authorisation of the retention and use of BPDs falling within a class BPD warrant 36
7 Safeguards 38
Storage 38
Safeguards before a BPD is made accessible 39
Access and examination 39
Personnel security 41
Additional access safeguards for confidential information relating to sensitive professions 41

Selection for examination of protected data relating to a member of a relevant legislature and constituency business 42
Material subject to legal privilege 43
Selection of legally privileged protected fields for examination 43
Handling, retention and deletion 45
Dissemination 45
Reporting to the Commissioner 46
Selection for examination of confidential journalistic protected data and journalists' sources 46
Offence of breaching examination safeguards 48
Review of retention and deletion 49
Destruction 49
Other management controls 50
8 Record-keeping and error-reporting 51
Errors 53
Serious errors 55
9 Oversight 57
10 Complaints 59
Annex A 60
The Security Service Act 1989 and the Intelligence Services Act 1994 60
The Counter-Terrorism Act 2008 61
The Human Rights Act 1998 61
The Data Protection Act 1998 61
Annex B – urgent authorisation process 63

1 Introduction

1.1 This code of practice relates to the exercise of functions conferred by virtue of Part 7 of the Investigatory Powers Act 2016 (“the Act”). It should be read alongside Part 7 of the Act and the explanatory notes. It provides guidance on the procedures that must be followed before bulk personal datasets can be retained and examined by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (“the intelligence services”). This code of practice is intended for use by the intelligence services.

1.2 The Act provides that all codes of practice issued under Schedule 7 to the Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, it mayt be taken into account.

1.3 For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of a intelligence service’s internal advice or guidance.

1.4 The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

1.5 Amongst the qualified rights is a person’s right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the intelligence services seek to obtain personal information about a person by selecting for examination bulk personal datasets. Other rights may also be engaged, such as the right to freedom of expression (Article 10).

1.6 Persons with access to BPDs 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 where systems or policies are updated.

2 Scope and definitions

2.1 The intelligence services 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 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 that has been obtained by an intelligence service 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 intelligence services 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 199 of the Act specifies that an intelligence service "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 holds the BPD electronically for analysis in the exercise of those functions.

2.4 As section 220 makes clear, the initial examination enables the intelligence service, when it comes into possession of a dataset, to carry out a preliminary examination of the contents with a view to establishing whether it is a BPD, and whether that dataset is of a nature that the intelligence service wish to retain and/or examine it. If so, the intelligence service 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.

2.5 This initial examination may only be carried out by an intelligence service for these limited purposes, and not for the purposes of any intelligence investigations or operations. An initial examination can include processing a set of information which might otherwise meet the definition of a BPD, with a view to permanently deleting all the individuals within that dataset who are not, and are unlikely to become, of intelligence interest. Any such processing must be completed within the relevant time period for initial assessment and no intelligence investigations or operations may be conducted as part of this processing until either the set of information has been processed such that it no longer meets the definition of a BPD; or a BPD retention and examination warrant has been issued.

2.6 An intelligence service should complete this initial examination as soon as reasonably practicable. What is 'reasonably practicable' will depend on many different factors. In cases where the intelligence service comes into possession of a BPD which has been created outside of the UK, there may be a period of time before the intelligence service 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 220(4) specifies that in cases of BPDs created outside the UK, the acquiring intelligence service 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 intelligence service has three months from the date on which the Head of the intelligence service 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 220(5) makes it clear that an intelligence service is not in breach of the requirement for a warrant to retain a BPD for the period between deciding (as part of the initial examination) that it wants to retain a BPD and the determination of intelligence service's application for a specific BPD warrant for that BPD. This allows an intelligence service 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 or to apply for a new class warrant. This is most likely to occur where a BPD is unsolicited (i.e. one which the recipient intelligence service has not requested or sought to obtain), because an intelligence service 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 intelligence service should complete its initial examination of the BPD and apply for a relevant warrant within the timeframes referred to in section 220(4) (and described in paragraph 2.7 above). Pending the relevant warrant being issued, the BPD may not be examined 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[1] ("DPA" – see also paragraph 7 and subsequent paragraphs of Annex A), which defines 'personal data' as follows:

> 'personal data means any data which relate to a living individual who can be identified –
>
> a) from those data; or
>
> b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

[1] The definition of "personal data" in the Data Protection Act 1998 will be replaced by a new definition provided for in section 2(2) of the Data Protection Bill which is currently before parliament and is expected to be commenced in 2018.

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 The definition of personal data in the Investigatory Powers Act includes data relating to deceased individuals. Bulk personal datasets may contain details about individuals who are deceased. 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 an intelligence service in the exercise of its statutory functions. If a BPD contains information about individuals who are known to be deceased, the relevant intelligence service may still 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. 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.

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 (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 <u>not</u> apply to BPDs obtained by an intelligence service when it is exercising a power under a warrant or other authorisation issued or given under the Investigatory Powers Act 2016, for example, warrants under Part 2, 5 or 6. BPDs 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 3.5 below). This is unless the intelligence service successfully applies to the Secretary of State to give a direction, with Judicial Commissioner approval, to disapply that regime in order to apply the Part 7 regime – see section 225 and paragraph 3.6 below. Once under the Part 7 regime, the provisions of this code of practice will apply.

3 BPDs – 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 200 of the Act provides that an intelligence service may not exercise a power to retain or examine a BPD unless this is authorised by a warrant under Part 7 of the Act.

Types of warrant that may be issued

3.2 Section 200(3) describes the two types of warrant provided for by Part 7: a '**class BPD warrant**' authorising an intelligence service to retain, or to retain and examine, BPDs that fall within a class described in the warrant; and a '**specific BPD warrant**' authorising an intelligence service to retain, or to retain and examine, the particular BPD described in the warrant.

3.3 A specific or a class warrant may authorise the retention of a BPD (or BPDs as the case may be), or the retention and examination of a BPD (or BPDs). An intelligence service is likely to seek a warrant to retain a BPD (or BPDs) in circumstances where the BPD that it has obtained is thought to be likely to be operationally useful, but further work is required before the BPD will be capable of being examined; or where the BPD must be retained for other reasons, but the intelligence service does not wish to select data from it for examination.

3.4 Where a warrant for retention only has been sought by an intelligence service, they may need more time beyond the initial examination period to establish the intelligence value of the data within the BPD in line with the purposes for which the retention has been sought. Where examination of the BPD may be required for this, a retention and examination warrant must be sought.

Exception to general requirement for authorisation by warrant

3.5 Section 201 explains the specific circumstances in which the general requirement under section 200 for a BPD warrant does not apply. Section 201(1) provides that the Part 7 authorisation scheme does not apply to BPD when this is obtained by an intelligence service by the exercise of **other** powers under the Act, for example, under a targeted or bulk interception or equipment interference warrant or under a bulk acquisition warrant (for bulk communications data). 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.

3.6 However, under section 225, an intelligence service 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 provisions of Part 7 of the Act applied instead. Such a direction can only be given with the approval of a Judicial Commissioner. Such a direction can also be varied by the Secretary of State, but again only with the approval of the Judicial Commissioner. Where an application for a direction under section 225 is made by the Head of an intelligence service, 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 a BPD that would require a specific warrant under Part 7. Under section 225(13), the Secretary of State may issue a specific warrant at the same time as giving a direction under this section.

3.7 In giving 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 given (with or without modifications). Therefore, in making an application for a direction, an intelligence service 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.

3.8 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 56 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act proceedings (see section 225(6)(a)). Nor may such a direction disapply sections 57-59 of the Act, which impose further restrictions on the disclosure of such material and make it an offence to make an unauthorised disclosure of the existence of an intercept warrant or any intercepted material (see section 225(6)(b)).

3.9 Section 201(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 intelligence service to hold, temporarily, a 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 intelligence service 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.

3.10 Section 201(3) makes clear that other sections of Part 7 of the Act also provide for exceptions from the requirement to obtain a warrant in particular circumstances. These relate: to cases where the Judicial Commissioner has

failed to approve an urgent specific BPD warrant but has imposed conditions as to the use or retention of the BPD (section 210(3)(b) – see paragraph 5.37 below); to a time-limited period in which an intelligence service is conducting an initial examination of a potential BPD (section 220(5) – see paragraph 2.3 above and subsequent paragraphs); and to a limited period after the non-renewal or cancellation of a warrant (section 219 – see paragraph 5.62 and subsequent paragraphs).

3.11 No interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. Section 2 of the Act requires a public authority to have regard to the following when issuing, renewing, cancelling or modifying a warrant under Part 7 of the Act:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means;
- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems, and
- any other aspects of the public interest in the protection of privacy.

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 intelligence services. 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 the decision to do so has been approved by a Judicial Commissioner (see paragraph 5.28 and subsequent paragraphs). A Judicial Commissioner will have access to the same application for a warrant as the Secretary of State.

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 5.33 and subsequent paragraphs). Even where the urgency procedure is followed, the Secretary of State must personally take the decision to issue the warrant. In any case where the Secretary of State decides to issue a specific warrant (whether under the urgency procedure or otherwise), he or she must personally sign the warrant unless it is not reasonably practicable to do so, in which case a designated senior official can sign the warrant. 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 intelligence service making the application. This involves consideration as to whether the application is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the 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 proportionate and whether the examination of the BPD is necessary for the operational purposes specified in the application (on which see paragraph 5.7 and subsequent paragraphs).

4.5 When completing a warrant application, whether for a specific BPD warrant or a class BPD warrant, the intelligence service must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular all reasonable efforts should be made to take account of information which weakens the case for the warrant. The review of the application should ensure that consideration has been given as to whether access to the dataset or datasets, while they are retained under the specific or class warrant (as the case may be), may be made available to any other intelligence service or an

international partner where it is necessary and proportionate to do so. If so this consideration should be included in the warrant application.

4.6 There may be circumstances in which an intelligence service may consider it appropriate to apply for a warrant to retain a BPD before it has physically acquired that BPD.

Class BPD warrants

4.7 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 an intelligence service to acquire travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.

4.8 Before submitting an application for a class warrant to the Secretary of State, the intelligence service 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 section 204 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;

- where the warrant would authorise examination, whether the 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 section 204 of the Act; and

- examining and retaining BPDs within that class is **proportionate** to what is sought to be achieved; 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.

4.9 Section 204(4) makes clear that the fact that the information that would be obtained under the warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

Applications for class BPD warrants

4.10 Section 204 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 BPDs to which the application relates; and

- if the intelligence service wishes to examine BPDs of that class, a list of the "operational purposes" for which the relevant intelligence service wishes to examine BPDs falling within that class.

Restriction on use of class BPD warrants

4.11 Section 202 provides that an intelligence service may not retain, or retain and examine, a BPD in reliance on a class BPD warrant if the Head of the intelligence service considers that:

(a) the BPD consists of, or includes, **protected data**;

(b) the BPD consists of, or includes, **health records;**

(c) a substantial proportion of the BPD consists of **sensitive personal data**; or

(d) the nature of the BPD, or the circumstances in which it was created, is or are such that its retention, or retention and examination, raises **novel or contentious issues** which ought to be considered by the Secretary of State and a Judicial Commissioner on an application by the head of the intelligence service for a specific BPD warrant.

4.12 'Protected data' is defined in section 203 of the Act. Additional guidance and requirements in respect of BPDs which comprise or include protected data is set out in paragraph 4.43 and following paragraphs. 'Health record' is defined by section 206(6) to mean a record, or a copy of a record, which (a) consists of information relating to the physical or mental health of an individual, (b) was made by or on behalf of a health professional in connection with the care of that individual, and (c) was obtained by the intelligence service from a health professional or a health service body or from a person acting on behalf of a health professional or health service body in relation to the record or the copy. 'Sensitive personal data' for the purposes of the Act is as defined in section 2 of the Data Protection Act 1998[2] but includes data relating to deceased individuals: see paragraph 8 of Annex A below.

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. A 'sensitive profession' for these purposes

[2] The definition of "sensitive personal data" in the Data Protection Act 1998 will be replaced by a new definition of "sensitive processing", which for intelligence services processing will be provided for in Part 4 of the Data Protection Bill which is currently before parliament and is expected to be commenced in 2018.

includes lawyers[3], doctors, journalists, Members of a relevant legislature, and Ministers of religion. (References to Members of a relevant legislature include a Member of either House of the UK Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly and Member of the European Parliament elected for the United Kingdom (see paragraph 7.15 and subsequent paragraphs)).

4.14 In particular, information relating to a member of a sensitive profession is not, in and of itself, considered confidential. For example, it 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 There are two scenarios in which the examination of a BPD could give rise to the need for additional protection for confidential information relating to members of sensitive professions.

4.16 First, it is possible that a BPD which contains **protected data** could include confidential information relating to a member, or members, of a sensitive profession. In this context, confidential information would include the content of communications between the professional, acting in their professional capacity, and another party. Thus, for example, it would include the content of communications between lawyer and client, doctor and patient, or MP and constituent. Such protected data could also include confidential information which identified a journalistic source.

4.17 In those circumstances, by virtue of the fact that the BPD contains protected data (and in accordance with section 202), the intelligence service must seek a specific warrant. The intelligence service must also apply the specific safeguards which apply to BPDs containing confidential information relating to members of sensitive professions, described in chapter 7 of this code, and comply with any additional conditions that are imposed by the Secretary of State before the protected data which is subject to the conditions is selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of selection.

4.18 Secondly, there is a small possibility that selection for examination of data (whether or not it is protected data) from BPDs could reveal the sources of journalistic material. In circumstances where the selection for examination conducted by an authorised person is for the purpose of identifying a source of journalistic material, the safeguards set out in Part 7 of this code must be applied.

[3] See paragraph 7.21 and subsequent paragraphs for specific safeguards in respect of legal professional privilege (LPP). In practice, LPP will only arise in the case of 'protected data', and so a BPD containing LPP will in any event be caught by the specific provisions in the Bill on such data: namely, a statutory prohibition on the use of class warrants and requirement to apply for a specific warrant, coupled with a power for the Secretary of State to attach conditions where 'UK content' is selected for examination, and specific access controls for intended/expected selection for examination of LPP.

Applications for specific BPD warrants

4.19 Section 205 provides for two sets of circumstances in which an intelligence service 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 intelligence service should make an application for a specific warrant.

4.20 In the '*Case 1*' scenario, the dataset does not fall within the scope of an existing class BPD warrant (and the intelligence service does not consider that it is appropriate to apply for a class BPD warrant that would cover that BPD, or is prevented from doing so).

4.21 In the '*Case 2*' scenario, the dataset falls within a class of BPD authorised by an existing class warrant, but either (i) the intelligence service is prevented by section 202 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraph 4.12 above) or (ii) the relevant intelligence service nevertheless considers that it would be appropriate to seek a specific BPD warrant.

4.22 In general, it is expected that there will be very few scenarios where an intelligence service is likely to consider it necessary to apply for a specific warrant, rather than a class warrant, other than in circumstances where the intelligence service is required to apply for a specific warrant under section 202.

4.23 However, the sorts of scenarios which may lead an intelligence service to apply for a specific warrant (otherwise than where required) include:

- where the intelligence service considers that there are issues which are specific to that particular BPD which would require particular consideration by the Secretary of State (for example, in relation to source protection or capability); and
- where retaining and examining the BPD is likely to give rise to particular political concern.

4.24 Where section 202 applies, the intelligence service is required by section 205 to include in its application for a specific BPD warrant an explanation of why it is prevented from retaining, or retaining and examining, the BPD in reliance on a class warrant, i.e. it must explain whether this is because the dataset consists of, or includes, protected data or health records, or because it includes a substantial proportion of sensitive personal data, or because it raises novel or contentious issues. This should not simply refer back to the statute: it should provide a more detailed explanation of the nature and extent of the material in question, to aid the Secretary of State's understanding of the dataset and the warrant application.

4.25 In the case of a dataset which includes a substantial proportion of sensitive personal data, in its application for the specific BPD warrant the intelligence service should describe the nature and extent of sensitive personal data in the dataset, where possible by reference to the different categories of sensitive

data set out in section 2(a)-(f) of the Data Protection Act 1998[4] (see paragraph 8 in Annex A).

4.26 If required in an individual case, the intelligence service can seek guidance from the Secretary of State and / or a Judicial Commissioner on whether it would be appropriate for a specific BPD warrant to be sought. The intelligence service should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

4.27 Section 205 specifies that an application for a specific BPD warrant must include:

- a description of the specific dataset to which the application relates; and
- a list of the "operational purposes" for which the relevant intelligence service wishes to examine the BPD (where the intelligence service seeks a warrant for retention and examination, rather than retention only).

4.28 An intelligence service should specify in the warrant application , when applying for a specific BPD warrant in respect of a particular BPD ('dataset A'), that it also wishes the authorisation to 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.

4.29 Before submitting an application for a specific warrant to the Secretary of State, the intelligence service must be satisfied that:

- retention of the BPD is **necessary** for one or more of the statutory purposes specified in section 205 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;
- where the warrant authorises examination, that the 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 205 of the Act; and
- examining and retaining the BPD in question is **proportionate** to what is sought to be achieved by the conduct.

4.30 Section 205(7) makes clear that the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

[4] The definition of "sensitive personal data" in the Data Protection Act 1998 will be replaced by a new definition of "sensitive processing", which for intelligence services processing will be provided for in Part 4 of the Data Protection Bill which is currently before parliament and is expected to be commenced in 2018.

BPDs containing 'protected data' – further restriction on class warrants and provision for attaching conditions to specific warrants

Background

4.31 Part 7 does not regulate a technique for acquiring information, but rather a species of data that may be acquired from a variety of different sources and by different methods, as set out in chapter 2 of this code. This fact means that, to the extent that the retention and examination of BPDs may be regarded as a capability, it is one that is of a different nature and kind from the techniques of bulk interception and bulk equipment interference.

4.32 Where data are acquired via bulk interception or bulk equipment interference, the degree of intrusiveness of the data falling into the protected class will depend on the nature and variety of the communications or items of information that are obtained from the systems or equipment in issue. It may therefore be difficult for the intelligence service implementing the warrant to assess in advance the nature and intrusiveness of all the data falling into the protected class that may be obtained by means of the bulk warrant. The Act must therefore apply the most stringent access controls to the selection for examination of all protected material relating to an individual known to be in the British Islands at the time of the selection. The statutory framework governing bulk interception and bulk equipment interference accordingly requires an intelligence service to obtain a targeted examination warrant when selecting for examination any protected material obtained under the warrant relating to an individual known to be in the British Islands at the time of the selection.

4.33 By contrast, where an intelligence service obtains a set of information other than in exercise of a power conferred by the Act, the intelligence service must conduct an initial examination to determine whether the set of information constitutes a BPD. If the set of information is retained as a BPD, the intelligence service will therefore be better able to assess the nature and intrusiveness of any data in the dataset that fall into the protected class. In particular, the intelligence service should be able to identify the presence and general nature of protected data that comprise the contents of e-mails, letters or other documents. It will accordingly be possible for the Secretary of State and the Judicial Commissioner, at the time a specific BPD warrant is issued, and having regard to the intelligence service's initial examination and assessment, to determine the safeguards that should apply to the selection for examination of protected data relating to an individual known to be in the British Islands up to, and including, a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

4.34 The stringent selection for examination safeguards that the Secretary of State must ensure are in place under section 221 of the Act will already be sufficient to regulate the vast majority of cases where data contained in a BPD is selected for examination. These safeguards ensure that any selection for

examination of data contained in a BPD is carried out only for the operational purposes specified in the warrant (which have been approved by the Secretary of State and Judicial Commissioner "double lock"). In addition, the selection of any such data for examination must be necessary and proportionate in all the circumstances.

4.35 Given the range and variation in intrusiveness of protected data contained in BPDs, it is not necessary or appropriate to apply additional controls to the selection for examination of all protected data in BPDs relating to an individual known to be in the British Islands at the time of the selection. Nor is it feasible for the Act to seek to identify all the various types of protected data that may be contained in BPDs, or to provide in detail for the limitations on access to each type of field depending on its relative intrusiveness, over and above those already mandated in section 221.

4.36 This chapter of the code accordingly sets out a scheme that enables the Secretary of State to impose additional controls in relation to the selection for examination of any protected data in the dataset relating to an individual who is known to be in the British Islands at the time of the selection. The scheme applies on a dataset by dataset basis having regard to the range of factors set out below, including the nature and intrusiveness of the protected data in the dataset.

Categorising data in a BPD

4.37 When categorising data contained in a BPD, the intelligence services should first consider whether the dataset as a whole comprises data that are not "private information" (see paragraph 4.42). For example, a dataset consisting of data which are publicly accessible online, for example from a telephone directory or Companies House, which is commonly used and known to be accessible to all, could be categorised as non-private information, in circumstances where there is no expectation of privacy over that information. There is less likely to be an expectation of privacy where data have been posted online and the purpose is to communicate that information to a wide audience. Information posted on personal social network sites normally accessed by a smaller circle of personal contacts, is likely to include private information to which an expectation of privacy would apply. No data fields in non-private datasets are protected data for the purposes of Part 7.

4.38 Except where paragraph 4.37 applies, the intelligence service should approach categorisation by determining whether the data contained in the BPD are systems data or identifying data (or both) and, if not, whether the data are not private information. These definitions are explained further below. Data that are systems data, identifying data or non-private are not protected. In cases where the intelligence service's initial examination of the BPD suggests that data within the dataset are the contents of letters, e-mails or other documents, then the intelligence service should assume that the BPD contains protected data (though that does not mean that all the data contained in that BPD are protected).

4.39 **Identifying data** in a BPD is data that may help to identify persons, systems, services, locations or events. Identifying data in a BPD does not therefore, of

itself, need to identify a person, system or service etc. For example, a person's name, address, occupation, dietary preferences and country of birth in a BPD will all be identifying data, even though any one of them, on its own, might not identify that person. An individual data item within a dataset (such as a single entry sentence or word) which meets these conditions can be categorised as identifying data in its own right. The majority of non-protected data in a BPD are likely to be categorised as identifying data.

4.40 **Systems data** is any data that enables or facilitates the functioning of any system or service. It includes all data that a system requires to function and provide its services. For example, if a passport number in a flight booking system has to be valid for the passenger to be able to fly then that passport number, when included in a travel BPD, will be systems data. The passport number will also be identifying data.

4.41 Where a data field is correctly classified as systems data because the operation of the system or service is dependent on the validity of the value of that field, the data field should be permanently categorised as systems data. That remains the case even if the dataset containing the systems data field is passed to a third party and is retained on a different system.

4.42 **Private information** includes information relating to a person's private or family life. In the BPD context, information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, commercial subscription databases, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data may also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

4.43 **Protected data** in relation to a BPD is any data contained in a BPD other than data which is one or more of the following:

- identifying data (see paragraph 4.39),
- systems data (see paragraphs 4.40 – 4.41), or
- data which is not private information (see sections 203 and 263(2) - (4) of the Act).

4.44 Protected data may contain data items that individually:

- fall within the definition of identifying data (see section 263(2) - (3));
- are capable of being logically separated from the BPD or the other data in the BPD; and
- if they were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the BPD or that other data, disregarding any meaning arising from the existence of the BPD or the other data or from any data relating to that fact.

4.45 If an individual data item meets these conditions then it should be categorised as identifying data in its own right – whilst the categorisation of the protected data from which it was derived remains unaffected.

Requirement to apply for a specific warrant for BPDs containing protected data

4.46 Where, to the best of the relevant intelligence service's knowledge or belief (and having regard to paragraph 4.37 above), it considers it likely that a BPD that it wishes to retain contains any protected data, it must apply for a specific warrant.

Additional range of factors to be included in the specific BPD warrant application

4.47 The warrant application in a case falling within paragraph 4.46 above should also contain as much information, and be as specific as is practically possible, in relation to the protected data in the BPD, including **the nature and type of the data and any other factors that may be relevant when assessing the level of intrusiveness of the protected data**. This is with a view to ensuring that the Secretary of State can:

- assess whether the arrangements in force in compliance with section 221 are sufficient for the selection for examination of protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection; and
- if the safeguards in section 221 are not sufficient, attach conditions to the warrant in accordance with section 207 of the Act.

4.48 In particular, the application for a specific warrant in such a case should include (so far as reasonably practicable) the following specific information:

- a description of the structure and scope of the BPD and of the information contained within it, including the different data involved and the nature and categories of data captured in those data, and, in particular, whether those data contain confidential information relating to members of sensitive professions (including whether the information is legally privileged[5]);
- a description, to include as much detail as is practically possible, of the nature and extent of the data which, following the relevant intelligence service's initial examination of the dataset, it is known or believed may contain protected data;
- whether any of the protected data are the contents of e-mails, letters or other documents;
- whether any of the protected data contain communications between a member of a relevant legislature (as defined in sections 26 and 111) and another person on constituency business;

[5] The additional safeguards that apply when an intelligence service wishes to select for examination data which contains confidential information relating to members of sensitive professions (including legally protected fields) are set out in chapter 7 of this code.

- any other factors that may be relevant to the Secretary of State's assessment of the level of intrusiveness of the protected data in the BPD (and therefore of the adequacy of the section 221 and where relevant, chapter 7 safeguards), including the extent of the expectation of privacy arising from the circumstances and context in which the protected data were included in the BPD;
- the intelligence service's assessment of whether, having regard to the above factors, the specific warrant should be issued unconditionally or only subject to such conditions as may be approved by the Secretary of State.

Authorising specific warrants for BPDs containing protected data

4.49 When considering a warrant application for any dataset falling within paragraph 4.46 above, the Secretary of State must determine, in the light of the **range of factors** set out in paragraphs 4.47 and 4.48 above, whether the Secretary of State is satisfied that the arrangements in force in compliance with section 221 would be sufficient for the selection for examination of the protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection. The section 221 safeguards are likely to be adequate and sufficient to provide the necessary Article 8 protections in cases where the BPD comprises a dataset containing protected data of a low level of intrusiveness (for example, protected data contained in a travel BPD provided by a prospective traveller to a service provider or in an internet dataset with minimal privacy settings which is accessible by a very large user group).

4.50 Where the Secretary of State is satisfied that the selection for examination safeguards are sufficient, the Secretary of State may issue the warrant without conditions.[6]

4.51 Where the Secretary of State is not so satisfied, but would otherwise be minded to issue the warrant (subject to the approval of the Judicial Commissioner), the Secretary of State may by virtue of the power conferred by section 207 of the Act **attach conditions** to the issue of the warrant in the way set out in paragraphs 4.52 to 4.55 below. In cases where the dataset contains the contents of letters, e-mails and documents, the Secretary of State will ordinarily require the intelligence service to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

Conditions which may be attached to the warrant in the exercise of the Secretary of State's discretion

4.52 Where the Secretary of State determines under paragraph 4.51 above that the selection for examination safeguards set out in section 221 would not be adequate and sufficient, the Secretary of State may attach conditions to the warrant when:

[6] Note that certain conditions will automatically apply in relation to some BPDs containing confidential information relating to members of sensitive professions, in accordance with chapter 7 of this Code.

- an intelligence service wishes to select for examination any protected data contained in the BPD using criteria referable to an individual known to be in the British Islands at that time, and
- the purpose of using those criteria is to identify protected data relating to that individual.

4.53 In such a case the Secretary of State may impose such requirements as the Secretary of State considers appropriate. Requirements may be suggested by the intelligence service. These may include – but are not limited to – one or more of the following requirements:

- to obtain the prior written approval of the Secretary of State and the Judicial Commissioner;
- to seek the prior approval of a senior manager in the relevant intelligence service and, if the Secretary of State considers appropriate, subject to the condition that the senior manager in question is independent of the investigation, operation or analytic work to which the selection for examination relates;
- to seek the prior approval of a senior official acting on behalf of the Secretary of State; or
- a prohibition on selecting for examination any protected fields in the BPD using criteria referable to an individual known to be in the British Islands at the time of the selection (and a determination, on that basis, that the section 221 safeguards are adequate and sufficient).

4.54 Where the dataset contains protected data of differing levels of intrusiveness, or a range of data, only some of which contains confidential information relating to members of sensitive professions, and the Secretary of State considers that only some of those data require the additional controls, (or that a range of additional controls is required), the Secretary of State may choose either (a) to apply the additional controls only to those data which require the additional controls or (b) to apply the additional controls to all the protected data contained in the dataset.

4.55 Where a “prior approval” condition of the kind referred to in paragraphs 4.52 or 4.53 is attached to the warrant, the prior approval may relate to individuals who are members of a group who share a common purpose or who are carrying on a particular activity, or may relate to more than one individual person where the authorisation is given in the context of a single operation or investigation or by reference to one or more specified areas of the relevant intelligence service’s operational activity.

Renewals of specific BPD warrants

4.56 When applying for **the renewal of a specific BPD warrant** containing protected data, the relevant intelligence service should inform the Secretary of State of the extent to which any protected data in the dataset have, since the issue or last renewal of the warrant, been selected for examination using criteria referable to an individual known to be in the British Islands at that time.

4.57 In cases where the Secretary of State is minded to renew such a warrant, the Secretary of State may either (a) renew the specific BPD warrant with the

same conditions, or (b) renew the specific warrant with different conditions or no conditions.

BPDs containing unanticipated protected data

4.58 It is possible that cases may occasionally arise where an intelligence service discovers, following the selection for examination of data contained in a BPD retained pursuant to a BPD warrant, that the BPD contains protected data fields which were not identified as protected at the time of the initial examination or where there was an urgent need to issue the warrant. Where such cases arise, the intelligence service must apply for a specific BPD warrant as soon as reasonably practicable in accordance with the procedure set out at paragraphs 4.46 to 4.55. The intelligence service must also ensure, as soon as reasonably practicable, that any selection for examination of the protected data in the BPD using criteria referable to an individual known to be in the British Islands ceases, until such time as the specific BPD warrant has been issued.

5 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 204 (class BPD warrants) or 205 (specific BPD warrants) if the Secretary of State considers the following tests are met:

- The warrant is necessary:[7]
  - 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 204(3)(a) or section 205(6)(a). (See paragraph 5.6 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).
- Except where a specific warrant is issued in an urgent case, a Judicial Commissioner has approved the decision to issue the warrant (see paragraph 5.28 and subsequent paragraphs).

5.2 In addition to the above points, when considering whether to issue a class BPD warrant, the Secretary of State will have regard to:

- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class and the necessity and proportionality considerations; and

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

- the number of individual bulk personal datasets which are likely to fall within that class warrant. In particular, the Secretary of State will not issue the warrant unless satisfied that it will be possible for the Secretary of State and Judicial Commissioner to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.

5.3 In the event that the Secretary of State is not satisfied in relation to either the nature and scope of the class, or the number of BPDs likely to fall within the class, the Secretary of State may either decline to issue the warrant or may issue the warrant subject to conditions.

5.4 If the Secretary of State decides to issue the warrant subject to conditions, he or she may impose conditions which either require the boundaries of the class to be reduced and/or specify what the upper limit of BPDs in the class should be. Where the Secretary of State refuses to issue the warrant, he or she may instead invite the relevant intelligence service to split the class into smaller classes and submit revised applications for a smaller class BPD warrant or smaller class BPD warrants and (where appropriate) specific BPD warrants for any individual BPDs.

5.5 Section 2 of the Act requires the issuing authority to have regard to the following when issuing, renewing, modifying or cancelling a warrant:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means,
- whether the level of protection applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of that information, and
- any other aspects of the public interest in the protection of privacy.[8]

What are operational purposes?

5.6 Section 221 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 263 of the Act for general definitions in the Act).

5.7 Sections 221(1) and 221(2) make clear that selection for examination may only be carried out 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

[8] Section 2 of the Act also requires the issuing authority to have regard to the public interest in the integrity and security of telecommunication systems but the duty applies only so far as they are relevant. This would rarely be the case in the BPD context.

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 examination for an operational purpose can, where it is necessary and proportionate to do so, be used, disclosed and retained for any statutory purpose.

5.8 The intelligence services 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 bulk warrant needs to reflect this. New operational purposes will be required over time. Section 212 of the Act makes clear that the heads of the intelligence services must maintain a central list of all of the operational purposes which they consider are purposes for which BPD may be retained, or retained and examined. The maintenance of this list will ensure the intelligence services are able to assess and review all of the operational purposes that are, or could be, specified across the full range of their bulk warrants at a particular time to ensure these purposes remain up to date, relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council.

5.9 The central list of operational purposes will not be limited to operational purposes relevant to BPD warrants. This list must provide a record of all of the operational purposes that are specified, or could be specified, on any bulk interception, bulk acquisition, bulk equipment interference or BPD warrant and, as far as possible, the operational purposes specified on the list should be consistent across these capabilities. Some operational purposes on the central list will be consistent across the three intelligence services, although some purposes will be relevant to a particular intelligence service or two of the three, reflecting differences in their statutory functions.

5.10 Section 212 also makes clear that an operational purpose may not be specified on an individual BPD warrant unless it is a purpose that is specified on the central list maintained by the heads of the intelligence services. And before an operational purpose may be added to that list, it must be approved by the Secretary of State. In practice, the addition of one operational purpose to the list will often require the approval of more than one Secretary of State. For example, where an operational purpose is being added to the list that is likely to be specified on bulk warrants issued to each of the three intelligence services, that operational purpose will need to be approved by both the Home Secretary and Foreign Secretary.

5.11 Sections 204 and 205 make clear that operational purposes specified on a BPD warrant must relate to one or more of the statutory purposes specified on the warrant. However, section 212(8) makes clear that it is not sufficient for any operational purpose simply to use the wording of one of the statutory purposes. The Secretary of State may not approve the addition of an operational purpose to the central list – and therefore to any bulk warrants – unless he or she is satisfied that the operational purpose is specified in a greater level of detail than the relevant statutory purposes. Operational purposes must therefore describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that the BPD may only be examined for specific reasons.

5.12 Section 215 of the Act provides for a class or specific BPD warrant to be modified such that the operational purposes specified on it can be added to or varied. Such a modification is categorised as a major modification and must be made by the Secretary of State. The decision to modify must be approved by a Judicial Commissioner before the modification has effect. In such circumstances, the operational purpose must be one that has been approved by the Secretary of State for addition to the central list. If the Secretary of State has not approved the addition of the purpose to the list, the modification to the warrant (to add a new operational purpose) may not be made.

5.13 The Act therefore creates a strict approval process in circumstances where an intelligence service identifies a new operational purpose, which they consider needs to be added to a bulk warrant. The Secretary of State must agree that the operational purpose is a purpose for which selection for examination may take place, and that it is described in sufficient detail such that it should be added to the central list. In addition, the Secretary of State must also consider that the addition of that purpose to the relevant bulk warrant is necessary, taking into account the particular circumstances of the case, before making the modification, and the decision to add the operational purpose must also be approved by a Judicial Commissioner.

5.14 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 212 makes clear that it must also be reviewed on an annual basis by the Prime Minister, and it must be shared every three months with the Intelligence and Security Committee of Parliament.

5.15 The Act does not limit the number of operational purposes that may be specified in the warrant. Where necessary, a warrant may include all operational purposes currently in use by an intelligence service. BPDs are likely to have potential relevance and utility across the full range, or most, of an intelligence service's operations or investigations. Other than in exceptional circumstances, it will always be necessary for every BPD warrant application to require the full range of operational purposes to be specified in relation to the selection for examination of data contained in the BPD authorised under the warrant.

5.16 The analysis of bulk systems data and identifying data (referred to hereafter as non-protected data, which comprises the majority of data in a BPD) is one of the key means by which the intelligence services are able to discover and assess threats to the UK. This generally involves the aggregation of non-protected data from a wide variety of sources acquired under multiple bulk warrants. Such analysis allows the intelligence services to draw together fragments of information into coherent patterns which allow for the identification of those threats while at the same time minimising intrusion into privacy.

Necessity and proportionality

5.17 Where the retention or examination of a BPD involves an interference with an individual's rights under Article 8 (right to respect for private and family life) of the ECHR or with other ECHR rights that might be engaged depending on the

circumstances, 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 sections 204(3) and 205(6) 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.

5.18 The Secretary of State must also believe that the retention 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 a BPD be necessary?

5.19 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 intelligence services and the Secretary of State must consider why retaining or retaining and examining the bulk personal dataset is necessary for the statutory and operational purposes referred to in paragraph 5.1 above.

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

When will retaining or examining a BPD be proportionate?

5.21 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 intelliogence services and the Secretary of State must balance (a) the level of interference with the individual's right to privacy (and any other rights that might be engaged depending on the circumstances), 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.

5.22 The intelligence services 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 intelligence service and the Secretary of State must also consider whether there is a reasonable and less intrusive alternative that will still meet the proposed objective.

5.23 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 intelligence service'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.

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

Authorisation of a specific warrant: senior officials

5.25 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 application, either in writing or orally, to the Secretary of State, including considerations of necessity and proportionality. Where the case is being explained orally, the senior official must keep a written record of the conversation. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the issue of the warrant it must not be issued. When a warrant is issued in this way the warrant instrument must contain a statement to that effect.

5.26 That a warrant has been signed by a senior official, with the personal and express authorisation of the Secretary of State, does not mean that the warrant is an urgent warrant. That being the case, the Secretary of State's decision to issue the warrant must be approved by a Judicial Commissioner before the warrant can be issued. However, a case in which it is not reasonably practicable for the Secretary of State to sign the warrant may additionally be an urgent case. If so the warrant may be issued without prior Judicial Commissioner approval and section 209 will apply.

5.27 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.

Judicial Commissioner Approval

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

The Judicial Commissioner will have access to the same application for the warrant as the Secretary of State.

5.29 Section 208 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 204(3)(a) or section 205(6)(a). In reviewing these matters, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner must when carrying out the review comply with the duties imposed by section 2 (general duties in relation to privacy).

5.30 In accordance with the investigation and information gathering powers at section 235(2) of the Act there is an obligation on the intelligence services and warrant granting department to provide the Judicial Commissioner with information when the Commissioner seeks clarification in relation to a warrant application. Where a Judicial Commissioner is seeking additional information this should be sought via the warrant granting department in order to determine whether the requested information would also need to be considered by the Secretary of State.

5.31 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).

5.32 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

5.33 The Act makes provision (see sections 209-210) for cases in which a specific BPD warrant is required urgently. It is not possible to seek an urgent class BPD warrant.

5.34 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 their life is in imminent danger;
- A significant intelligence-gathering opportunity, which is significant because of the nature of the potential intelligence or because the operational need for the intelligence is significant, and 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 BPDs to identify the vessel to prevent the weapons reaching the terrorist.

5.35 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).

5.36 If the Judicial Commissioner approves the Secretary of State's issuing of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting intelligence service, 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.

5.37 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 intelligence service or the Secretary of State can make, or be required by a Judicial Commissioner to make, representations to the Commissioner about requirements to destroy datasets and/or conditions relating to use or retention.

5.38 An intelligence service is not to be regarded as in breach of the requirement to have a warrant where it retains or (as the case may be) examines a bulk personal dataset in accordance with conditions imposed by the Judicial Commissioner in the way described in paragraph 5.37 above.

5.39 If the Judicial Commissioner does not approve the urgent warrant, the relevant intelligence service 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.

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

Duration of BPD warrants

5.41 The duration of a warrant (other than an urgent warrant) is six months from the day it was issued, unless it is cancelled earlier. An urgent warrant lasts for five working days after the day on which it was issued. Warrants may only be renewed in the last 30 days of the period for which they have effect. Where a warrant is renewed, the six month duration begins on the day following the day on which it would otherwise have ceased to have effect.

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

Modification of a BPD warrant

5.43 Section 215 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 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 215. Once the modification comes into force, the added or varied operational purpose may be used to select for examination data from any BPD retained under that warrant, even if the BPD was acquired prior to the addition or variation of the operational purpose.

5.44 A modification to add or vary an operational purpose must be made by the Secretary of State (except in the situation described in paragraph 5.45 below), 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 5.48 and subsequent paragraphs for more on urgent modifications.) A modification to remove an operational purpose may be made by the Secretary of State or a designated senior official acting on behalf of the Secretary of State.

5.45 The decision to make a modification must be taken personally by the person making the modification and the instrument making the modification must be signed by that person. If it is not reasonably practicable for the Secretary of State to sign the instrument making a modification to add or vary an operational purpose – for example where he or she is out of the country, working within his or her constituency, or otherwise unavailable – a senior official acting on behalf of the Secretary of State may sign the modification instrument with the express authorisation of the Secretary of State. In such a case, the modification instrument must contain a statement (a) that it is not reasonably practicable for the instrument to be signed by the Secretary of

State and (b) that the Secretary of State has personally and expressly authorised the making of the modification.

5.46 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). The notification 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.

5.47 The modification instrument should be addressed to the person to whom the warrant was issued (i.e. the Head of the relevant intelligence service).

Urgent modification of a BPD warrant

5.48 Sections 215, 216 and 217 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 Judicial Commissioner must decide whether to approve the decision to make such a modification within three working days.

5.49 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 intelligence service 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.

5.50 Where a Judicial Commissioner refuses to approve the urgent modification, the Secretary of State may not refer the application to the Investigatory Powers Commissioner.

Renewal of BPD warrants

5.51 The Secretary of State may renew a warrant within the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect, with the approval of the Judicial Commissioner. Urgent warrants may be renewed at any point before their expiry date. 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 continues to be necessary to retain and/or examine the specific BPD(s) or the class of BPDs, and why this

continues to be proportionate. In addition, in relation to BPDs containing protected data, the applicant must give all the relevant information required to enable the Secretary of State to determine whether the same conditions should continue to apply (see, in particular, paragraph 4.56 above).

5.52 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 BPDs 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. In relation to BPDs containing protected data, the Secretary of State should consider, in addition, what (if any) conditions should be applied to the warrant (see paragraph 4.57 above)

5.53 When considering whether to renew a class BPD warrant, the Secretary of State will have regard to:

- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class and the necessity and proportionality considerations; and
- the number of individual bulk personal datasets which are likely to fall within that class warrant. In particular, the Secretary of State will not renew the warrant unless satisfied that it will still be possible for the Secretary of State and Judicial Commissioner, to continue to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.

5.54 In the event that the Secretary of State is not satisfied in relation to either the nature and scope of the class, or the number of BPDs likely to fall within the class, the Secretary of State may either decline to renew the warrant or may renew the warrant subject to conditions.

5.55 If the Secretary of State decides to issue the warrant subject to conditions, he or she may impose conditions which either require the boundaries of the class to be reduced and/or specify what the upper limit of BPDs in the class should be. Where the Secretary of State refuses to issue the warrant, he or she may instead invite the relevant intelligence service to split the class into smaller classes and submit revised applications for a smaller class BPD warrant or smaller class BPD warrants and (where appropriate) specific BPD warrants for any individual BPDs.

5.56 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 after the day at the end of which it would otherwise have ceased to have effect if it had not been renewed.

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

Cancellation of warrants

5.58 The Secretary of State, or a senior official acting on his or her behalf, may cancel a BPD warrant at any time (see section 218). Such persons must cancel a BPD warrant if, at any time before its expiry date, he or she is considers that:

5.59 the warrant is no longer necessary for any of the purposes for which a warrant may be issued;

5.60 the conduct is no longer proportionate to what is sought to be achieved;

5.61 where the warrant authorised examination, that the examination of dataset, or any datasets within that class, is no longer necessary for any of the specified operational purposes.

5.62 The intelligence services 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.

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

5.64 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

5.65 Section 219 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 201(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 intelligence service 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 219 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 intelligence service may apply for a new class or specific BPD warrant within five working days (section 219(2)).

5.66 If the relevant intelligence service 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 intelligence service 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 219(7), the intelligence service 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 intelligence service so applies, the Secretary of State can then direct that any of the material should be destroyed or, with the approval of a Judicial Commissioner, can authorise the retention or examination of any of the material for a period of up to 3 months, subject to such conditions as the Secretary of State considers appropriate. Retention or examination is lawful under such a direction. During that period, the intelligence service must consider whether to apply for a new warrant and then do so as soon as reasonably practicable and in any event within three months. Retention and examination remains lawful for the period between the intelligence service applying for a new warrant and the determination of that application, even if determination takes place after the end of the three month period.

5.67 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 intelligence service 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.

5.68 If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, section 219(5) 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 219(6)).

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

6.1 For the purpose of dealing with BPDs falling within the scope of an existing class BPD warrant, each intelligence service 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 intelligence service must be satisfied that:

- the BPD in question falls within the scope of the relevant class warrant;
- it is not prevented by section 202 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraph 4.11 and subsequent paragraphs);
- retention of the BPD is **necessary** for one or more of the relevant intelligence service'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 204(3)(a) or section 205(6)(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 retained 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 5.17 and subsequent paragraphs and of operational purposes at paragraph 5.6 and subsequent paragraphs.

6.4 Before a new dataset falling within the scope of a class BPD warrant is held electronically by an intelligence service for analysis in the exercise of its functions, the relevant persons with access to BPDs in that intelligence service should consider the factors set out in paragraph 6.2 above and complete the relevant formal internal authorisation procedure. Any application to a senior manager to retain datasets falling within the scope of a class warrant 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 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 intelligence service's legal advisers; and
- the extent of political, reputational or other risk.

6.5 Line or senior management within the intelligence service should be consulted for guidance, or the intelligence service may also seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant warrant-granting Department), the Secretary of State and/or the Investigatory Powers Commissioner. If the intelligence service is not clear on whether reliance on a class warrant is appropriate, then they should seek guidance from the Secretary of State and / or a Judicial Commissioner. The intelligence service 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 intelligence service, which will include the date of approval. Where relevant, this record should also contain the date when the intelligence service 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 7.53 and subsequent paragraphs).

7 Safeguards

7.1 This chapter sets out the safeguards which each intelligence service 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 intelligence service for storing BPD and for protecting the datasets from unauthorised disclosure are satisfactory (as set out in sections 204(3)(d) and 205(6)(d)). The Secretary of State must also ensure that certain arrangements are in place relating to the examination of bulk personal datasets as required by section 221.

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 a 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 datasets containing a substantial proportion of sensitive personal 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 intelligence service 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 BPD is effectively protected, that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that it is detected and that appropriate disciplinary action is taken. In particular, each intelligence service 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-clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Safeguards before a BPD is made accessible

7.4 Where a BPD contains either a substantial proportion of sensitive personal data[9] or confidential information relating to sensitive professions (see paragraph 4.13 and subsequent paragraphs), before such a BPD is held electronically by an intelligence service for analysis in the exercise of its functions the relevant intelligence service should consider whether access by persons 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 intelligence service 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 5.17 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 3 of Annex A);
- before accessing or disclosing information, individuals must also consider whether to do so would be proportionate (as described in paragraph 5.21 and subsequent paragraphs and below). For instance, they must consider whether other, less intrusive methods can reasonably 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;

[9] Such a dataset will be subject to a requirement to obtain a specific BPD warrant

- 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 can be issued.

7.6 No data may be selected for examination other than in accordance with specified operational purposes. In general, automated systems should, where possible, be used to effect the selection for examination in accordance with section 221 of the Act and the arrangements made by Secretary of State under that section for ensuring that any selection of data from the BPDs is carried out only for the specified operational purposes. A limited number of officials may also be permitted to access the system during the processes of processing and selection for examination, for example to check system health. Such access must itself be necessary on the grounds specified in sections 204(3)(c)(ii) and 205(6)(c)(ii). Where such access involves selection for examination of data, it must be necessary and proportionate for an operational purpose specified on the warrant. Intelligence service arrangements for access will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

7.7 In addition, no data may be selected for examination for the specified operational purposes unless this is necessary and proportionate in all the circumstances and unless the selection is in accordance with the arrangements the Secretary of State must ensure are in force under section 221 for ensuring this. These arrangements must include provisions relating to the creation and retention (for the purposes of subsequent examination or audit) of documentation outlining why access to the data by authorised persons is necessary and proportionate, and the applicable operational purposes.

7.8 Periodic audits should be carried out to ensure that the requirements set out in section 221 of the Act are being met. These audits must include checks to ensure that the documentation justifying the selection for examination has been correctly compiled and, specifically, that selection for examination of data was for an operational purpose that the Secretary of State considered necessary for examination. 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 breaches of safeguards must be reported to the Investigatory Powers Commissioner.

7.9 The intelligence services 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 persons with access to BPDs 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

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

Additional access safeguards for confidential information relating to sensitive professions

7.11 The intelligence services should ensure that, before intelligence service staff use a bulk personal dataset specifically with the intention of selecting for examination confidential information relating to members of sensitive professions, particular consideration is given to the necessity and proportionality justification for the interference with privacy that will be involved. Paragraphs 4.13 to 4.18 of this code gives further guidance on what is considered to amount to 'information relating to members of sensitive professions' for the purposes of this code. Where confidential or constituency business information is disseminated externally, reaonsable steps shold be taken to mark the disseminated information as confidential.

7.12 Searches for sources of journalistic information do not necessarily depend on the content of the BPD, but could in rare cases be facilitated by the examination of data within BPDs. Therefore, the safeguards that apply in relation to the identification of sources of journalistic material should be read as applying to any data which is selected for examination from a BPD by an intelligence service with the intention of identifying a source of journalistic material and not just those where this is done in relation to those BPDs which contain protected data.

7.13 Section 2 of the Act makes clear that due regard must be given to whether the level of protection applied in relation to any examination of a BPD is higher because of the particular sensitivity of that information. Examples of sensitive information include but are not restricted to legally privileged information, confidential journalistic material, the identity of a journalist's source, and communications between a member of the relevant legislature and their constituent.

7.14 However, where an authorised person selects data for examination with the intention of obtaining privileged or otherwise confidential information, the officer must give special consideration to necessity and proportionality and

must take into account any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken when considering whether data should be selected for examination in such circumstances, including additional consideration of whether there might be unintended consequences of such examination and whether the public interest is best served by the data being selected for examination. These protections do not apply where the communications in issue were made with the intention of furthering criminal purpose.

Selection for examination of protected data relating to a member of a relevant legislature and constituency business

7.15 Where:

- An intelligence service wishes to search (meaning select for examination) a BPD retained pursuant to a specific BPD warrant and the purpose of the search is to select for examination protected data relating to a member of a relevant legislature; and
- the specific warrant has been issued subject to a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner before such protected data is selected for examination;

the intelligence service must have obtained the prior approval of the Prime Minister

7.16 The prior approval of the Prime Minister must also be obtained if the intelligence service intends to select for examination protected data relating to a member of a relevant legislature who is outside the British Islands at the time of the selection for examination. Such approval should only be obtained once the Secretary of State has approved such examination.

7.17 “Member of a relevant legislature” for these purposes has the meaning given in sections 26 and 111 of the Act.

7.18 Where the intention is to acquire communications between a member of a relevant legislature and another person on constituency business the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the information is exchanged with a criminal purpose, for example, if the communications involve incitement to murder or to acts of terrorism, then the information will not be considered confidential for the purposes of the Act.

7.19 Where constituency business information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of the information, advice should be sought from a

legal adviser within the relevant intelligence service and before any further dissemination of the content takes place.

7.20 Any case where constituency business content is intentionally selected for examination and retained (separately from the BPD) should be notified to the Investigatory Powers Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any content which has been retained should be made available to the Commissioner on request.

Material subject to legal privilege

7.21 For the purposes of this code, any communication – whether in the UK or overseas - between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether the material is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant intelligence service.

7.22 Section 263(1) of the Act defines items subject to legal privilege.

7.23 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the legal adviser is acting unwittingly or culpably). But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, intelligence service or organisation qualified to do so, such as advocates, barristers, solicitors or Chartered Legal Executives.

7.24 Selecting legally privileged protected material for examination is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The selection for examination of legally privileged protected data contained in BPDs (whether deliberately or otherwise) is therefore subject to the additional safeguards set out in paragraph 7.25 and subsequent paragraphs of this code. The guidance set out may in part depend on whether the legally privileged protected data have been selected intentionally or incidentally to other data which have been sought.

Selection of legally privileged protected fields for examination

7.25 These paragraphs apply where an intelligence service wishes to search a BPD and:

- the purpose, or one of the purposes of the search, is to select for examination protected data subject to legal privilege, or

- the use of the relevant search criteria is likely to identify such data.

7.26 Where these paragraphs apply (and without prejudice to chapter 4 of this code), the intelligence service is prohibited from carrying out the search unless prior approval has been given by a relevant approver. The relevant approver in the case of a search relating to an individual known to be in the British Islands at the time of the selection is the Secretary of State, subject to the approval of the Judicial Commissioner. In any other case, the relevant approver is a senior official acting on behalf of the Secretary of State (i.e. a senior official in the Secretary of State's department, not a senior official within the intelligence service).

7.27 Before carrying out the search, the intelligence service must notify the relevant approver. Where the use of the search criteria is likely to identify legally privileged protected data, the notification to the senior official should include, in addition to the reasons why it is considered necessary for the selection for examination to take place, an assessment of how likely it is that legally privileged protected data will be selected. In addition, the notification should state whether the purpose, or one of the purposes of the search, is to select for examination legally privileged protected data. Where the intention is not to identify legally privileged protected data, but it is likely that such data will nevertheless be selected, that should be made clear in the notification, and the intelligence service should confirm that any inadvertently obtained privileged data will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to those data.

7.28 On receiving the notification, the relevant approver must decide whether to give an approval for the search to be carried out. The relevant approver may give an approval only if:

- the approver considers that the arrangements made for the purposes of section 205(6)(d) include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege, and
- where the first bullet of paragraph 7.25 applies, the approver considers that there are exceptional and compelling circumstances that make it necessary to authorise the search. Such circumstances will arise only in a very restricted range of cases, such as where necessary for the purpose of preventing death or serious injury or in the interests of national security, and the selection for examination is reasonably regarded as likely to yield intelligence necessary to counter the threat. The exceptional and compelling test can only be met when the public interest in obtaining the information outweighs the public interest in maintaining the confidentiality of legally privileged material, and where there are no other reasonable means of obtaining the information.

7.29 In the event that legally privileged protected data are inadvertently and unexpectedly selected for examination (and where the enhanced procedure set out above has consequently not been followed), any protected data so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged protected data may be intentionally selected for

examination by reference to the relevant search criteria unless approved by the relevant approver as set out in paragraph 7.28.

Handling, retention and deletion

7.30 Officials who examine protected data contained in BPDs should be alert to any data which may be subject to legal privilege.

7.31 Where it is discovered that legally privileged protected data have been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain them. If not, the protected data should be securely destroyed as soon as possible.

7.32 Where protected data have been identified following examination as legally privileged, each intelligence service should take steps to ensure that officials who have access to the bulk personal datasets in question are alerted to the fact that the dataset contains legally privileged material. The intelligence service should report to the Secretary of State and Judicial Commissioner on the fact that the dataset contains legally privileged material when it next applies for renewal of the BPD specific warrant in question.

7.33 In addition, where legally privileged protected data are recorded and retained separately from the bulk personal dataset for purposes other than their destruction they should be clearly marked as subject to legal privilege. Such data should be retained only where it is necessary and proportionate to do so. They must be securely destroyed when their retention is no longer needed for the authorised statutory purposes. If such data are retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for those purposes.

Dissemination

7.34 A legal adviser must, wherever possible, be consulted on the lawfulness (including the necessity and proportionality) of any proposed action on or further dissemination of protected data subject to legal privilege.

7.35 The dissemination of legally privileged protected data to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged protected data held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged protected

data in order to gain a litigation advantage over another party in legal proceedings.

7.36 In order to safeguard against any risk of prejudice or perceived abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or policy officials with conduct of legal proceedings should not see legally privileged protected data relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such content could yield a litigation advantage, the direction of the Court must be sought.

Reporting to the Commissioner

7.37 Where an item identified as subject to legal privilege following its examination is recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant intelligence service must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. Any legally privileged protected data that is retained should be made available to the Commissioner on request, including detail of whether those data have been disseminated. The Commissioner may direct that such data is destroyed or impose conditions as to its disclosure. The Commissioner must have regard to any representations made by the Secretary of State of the affected intelligence service about any such destruction or conditions imposed.

Selection for examination of confidential journalistic protected data and journalists' sources

7.38 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

7.39 Confidential journalistic material is defined in section 264 of the Act. The Act states that confidential journalistic material means:

a) in the case of material contained in a communication, journalistic material which the sender of the communication

   i. holds in confidence, or

   ii. intends the recipient, or intended recipient, of the communication to hold in confidence;

b) in any other case, journalistic material which a person holds in confidence.

7.40 Confidential journalistic material includes data acquired or created for the purposes of journalism and held subject to an undertaking to hold it in

confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

7.41 Section 264(7) sets out when a person holds material in confidence. This is if a person holds material subject to an express or implied undertaking to hold it in confidence or the person holds the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

7.42 A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Throughout this code any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.

7.43 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

7.44 Where material is created or acquired with the intention of furthering a criminal purpose, section 264(5) states that the material is not to be regarded as having been created or acquired for the purpose of journalism. For example, if a terrorist organisation is creating videos for the purposes of propaganda, and this material is created or acquired for the promotion or glorification of terrorism as prohibited by the Terrorism Act 2006, the material cannot be regarded as journalistic material for the purposes of the Act. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material. The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material as defined in the Act.

7.45 Where the intention is to select for examination any data in order to identify a source of journalistic information the approval of a person holding the rank of Director or above within their organisation should be obtained. The reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. Where the intention is to select for examination data in order to identify a source of journalistic information the public interest requiring such selection must override any other public interest.

7.46 Confidential journalistic protected data which have been identified as such, and data which identifies a source of journalistic information, should be retained only where it is necessary and proportionate to do so. It must be securely destroyed when its retention is no longer needed for those purposes. If such data are retained other than for the purposes of their destruction, there

must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate.

7.47 Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential journalistic protected data, advice should be sought from a legal adviser within the intelligence service and before any further dissemination of the content takes place.

7.48 In any case where confidential journalistic protected data following their examination are recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant intelligence service must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any data which has been retained other than for the purpose of its destruction should be made available to the Commissioner on request.

Offence of breaching examination safeguards

7.49 Data contained within a BPD may only be selected for examination subject to the safeguards in sections 221 to 223 of the Act. Section 224 of the Act makes it an offence for a person deliberately to select data for examination in breach of these safeguards where that person knows or believes such selection does not comply with the safeguards.

Disclosure

7.50 For the purposes of this paragraph, disclosure means providing a copy of a BPD or information held in a BPD to a third party. It does not cover third party access to BPDs via the electronic analysis systems of the intelligence service which holds the warrant. Such access will be governed as appropriate by the access and examination safeguards set out in paragraphs 7.5 and 7.6 of this code.

7.51 Disclosure of BPDs, or information in BPDs held by an intelligence service (whether acquired under class BPD or specific BPD warrants) is not generally regulated by the IP Act. In general, disclosure of BPDs, or information in BPDs, continues to fall to be regulated by sections 2(2)(a) and 4(2)(a) of the ISA, and section 2(2)(a) of the SSA, and by the arrangements made in accordance with those statutory provisions so as to ensure compliance (amongst other things) with the requirements of necessity and proportionality: see paragraph 3 of Annex A.

7.52 However, if BPDs have been obtained by the intelligence service under a warrant or other authorisation under the Act (see section 201(1)), subsections (5) and (6) of section 225 provide that in certain circumstances, conditions imposed under the Act could be read across from the acquisition regime, which have an impact on the extent of disclosure, or the requirements that must be met before disclosure can take place. In addition, some of the safeguards that apply in relation to confidential material relating to members of sensitive professions will apply where that material is shared.

Review of retention and deletion

7.53 Each intelligence service 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 intelligence service 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.

7.54 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 reasonably 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 dataset;
- 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

7.55 Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it held within the relevant intelligence service must be scheduled for destruction as soon as possible once it is no longer needed for any of the authorised purposes. Section 263 of the Act defines destroy for the purposes of the Act as deleting the data in such a way as to make access to the data impossible, for example by taking such steps as might be necessary to make the data unavailable or inaccessible to anaylsts or investigators pending destruction. No further steps such as physical destruction of hardware are required. Each intelligence service should report to the Secretary of State, on a six-monthly basis, with a list of all BPDs destroyed in the previous six months.

Other management controls

7.56 The retention and disclosure of a bulk personal dataset should be subject to scrutiny in each intelligence service, 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 a BPD is permitted only for the specified operational purposes and for the relevant intelligence service'sstatutory 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 intelligence service's statutory functions and is proportionate to achieving that objective.

7.57 Each intelligence service should ensure that there is a system in place whereby the relevant audit or user monitoring team effectively monitors the examination of bulk personal datasets by persons with access to BPDs in order to detect misuse or identify activity that may give rise to security concerns.

7.58 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.

7.59 All investigations are required to be reported 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 intelligence service 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 their 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;
- where the decision to issue a warrant is not approved by the Judicial Commissioner, the written response for refusal as given by the Judicial Commissioner;
- a record of whether, following a refusal to approve a decision to issue or renew a warrant by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner; and
- where there is such an appeal and the Investigatory Powers Commissioner also refuses to approve the decision to issue or renew the warrant, the written reasons given.

8.3 Each intelligence service 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 not approved 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 issue an urgent specific BPD warrant has subsequently not been approved by a Judicial Commissioner;
- the number of times approval has been given to select for examination protected data retained in reliance on a specific BPD warrant where selection of the data for examination is intended, or likely, to identify any items subject to legal privilege;
- the number of times approval has been given to select for examination protected data retained in reliance on a specific BPD warrant where selection for examination is intended to identify confidential journalistic data;
- the number of times approval has been given to select data for examination where the intention is to identify or confirm a source of journalistic information;
- the number of times approval has been given to select for examination protected data relating to a member of a relevant legislature;
- 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 and details of authorisations by the Secretary of State under section 219(3)(b) (relating to the non-renewal or cancellation of BPD warrants);
- the number and details of directions by the Secretary of State under section 225(3) (relating to the application of Part 7 to bulk personal datasets obtained under the Act);

- 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; and
- a record of BPDs held that fall within a particular class warrant (see chapter 6 above); anda list of all BPD destroyed in the previous six months (see paragraph 7.55).

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 intelligence services.

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.

Errors

8.6 This section provides information regarding errors. Proper application of the Investigatory Powers Act 2016 and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors.

8.7 Any failure by a public authority or such other persons providing assistance to apply correctly the process set out in this code will increase the likelihood of an error occurring. Wherever possible, technical systems should incorporate functionality to minimise errors. A person holding a senior position within each intelligence service must undertake a regular review of errors and a written record must be made of each review.

8.8 Section 231 of the Act makes specific reference to a **relevant error**, which is defined in section 231(9) of the Act as an error:

- by a public authority complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and
- of a description identified for this purpose in a code of Practice under Schedule 7.

8.9 An error occurs in one or both of the following circumstances:

- a BPD has been retained and/or examined without lawful authority;

- there has been a failure to adhere to the restrictions on the use or disclosure of material imposed by sections 221 to 223.

8.10 Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the Act, all relevant errors must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

8.11 When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error. A public authority that spots an error but may not have committed it is also under a duty to notify the Investigatory Powers Commissioner.

8.12 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the intelligence service responsible must also inform the Commissioner of when it was initially identified that an error may have taken place.

8.13 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the public authority that made the error, that report should also include: the cause of the error; amount of data retained or retained and examined; any unintended collateral intrusion; any analysis or action taken; whether the data has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

8.14 As set out at section 231(9) of the Act, the Commissioner will keep under review the definition of relevant errors. The Commissioner may also issue guidance as necessary, including guidance on the format of error reports. The intelligence services must have regard to any guidance on errors issued by the Investigatory Powers Commissioner.

8.15 This section of the code cannot provide an exhaustive list of possible errors that would fall within paragraph 8.9 above. However, examples could include:

- failing to seek a specific BPD warrant for a dataset which consists of or includes protected data, or health records, or is novel or contentious;
- failing to apply for a specific BPD warrant within the permitted period, unless retention is authorised by a class BPD warrant;

- failure to obtain the appropriate authorisation when the intention of the selection for examination is to identify items subject to legal privilege or the expectation is that such items will be identified;
- a material failure to adhere to the arrangements in force under section 221 of the Act, such as selecting data for examination from a BPD for a purpose not specified in the specific or class BPD warrant; and
- for a BPD falling within the scope of an existing class BPD warrant, a material failure to comply with the formal internal authorisation procedure required by paragraph 6.1 and subsequent paragraphs of this code.

8.16 Wherever possible, technical systems should incorporate functionality to minimise errors. A senior person within that organisation must undertake a regular review of errors.

8.17 Where an error occurs which is also considered to constitute an offence detailed in chapter 3 of this code, the provisions of this chapter must still be applied to the handling of the error

Serious errors

8.18 Section 231 of the Act states that the Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient for an error to be a serious error.

8.19 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- the seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
  - national security;
  - the prevention or detection of serious crime;
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any of the intelligence services.

8.20 Before making his or her decision, the Commissioner must ask the intelligence service which has made the error to make submissions on the

matters concerned. The intelligence services must take all reasonably practicable steps notified to them by the Investigatory Powers Commissioner to identify the subject of a serious error.

8.21 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

9 Oversight

9.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers contained within Part 7 of the Act and adherence to the practices and processes described by this code. The Commissioner 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 Commissioner will be supported by inspectors and others, such as technical experts and legal experts, qualified to assist the Commissioner in their work. The Commissioner will also be advised by the Technology Advisory Panel.

9.2 The Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative. Section 236 provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

9.3 The Commissioner 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 Commissioner must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (see section 229(6)). A Commissioner must in particular not jeopardise the success of the intelligence services, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces (see section 229(7)). In using these powers the intelligence services must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

9.4 Anyone, including anyone working for an intelligence service, who has concerns about the way that investigatory powers are being used, may report their concerns to the Commissioner. 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 relevant error of which he is aware. Here, relevant error has the meaning given by section 231(9). This may be in addition to the person raising concerns through the internal mechanisms within the public authority.

9.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to a person 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 person affected. Further

information on errors can be found in chapter 8 of this code. The public authority who has made the relevant error will be able to make representations to the Commissioner before the Commissioner decides it is in the public interest for the person to be informed. The Commissioner must also inform the affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal (see chapter 10 for more information on how this can be done).

9.6 The Investigatory Powers Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Commissioner's report.

9.7 The Investigatory Powers Commissioner may also report, at any time, on any of its investigations and findings as they see fit. The intelligence services may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

9.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: www.ipco.org.uk

10 Complaints

10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of certain investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the intelligence services. 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. Following receipt of a complaint or claim from a person, 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. A 'person' for these purposes includes an organisation and association or combination of persons (see section 81(1) of RIPA), as well as an individual.

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.

10.4 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

10.5 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.

Annex A

The Security Service Act 1989 and the Intelligence Services Act 1994

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.
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.
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 intelligence services to ensure that there are arrangements for securing (i) that no information is obtained by the relevant intelligence service 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).
4. SSA and ISA accordingly impose specific statutory limits on the information that each of the intelligence services 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

5. Section 19 of the **Counter-Terrorism Act 2008** confirms that 'any person' may disclose information to the intelligence services 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 intelligence services in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its other functions. 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

6. Each of the intelligence services is a public authority for the purposes of the Human Rights Act 1998. When obtaining, using, retaining and disclosing bulk personal datasets, the intelligence services 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. Other Convention rights, for example Article 6 (right to a fair trial) and Article 10 (freedom of expression), may be engaged depending on the circumstances. In practice, this means that any interference 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[10]

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

- 'personal data means any data which relate to a living individual who can be identified –

  a) from those data; or

  b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

  and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

[10] Or relevant Data Protection legislation as defined in section 2(9) of the Data Protection Bill, upon repeal of the Data Protection Act 1998

8. Section 2 of the DPA defines "sensitive personal data"[11] 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.

9. Each of the intelligence services is a data controller in relation to all the personal data that it holds. Accordingly, when the intelligence services use any BPDs 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).

[11] For the purposes of the 2016 Act, the definition of sensitive personal data only includes the data types listed at section 2(2)(a) to (f) of the Data Protection Act 1998, and excludes (g) the commission or alleged commission of any offence, and (h) any proceedings for any offence committed or alleged to have been committed, this disposal of such proceedings or the sentence of any couirt in such proceedings.

Annex B – urgent authorisation process