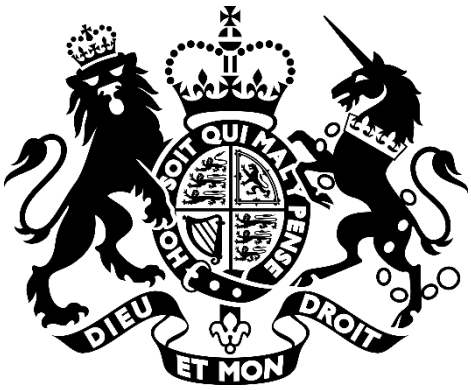
Home Office

Intelligence services' use of third party bulk personal datasets

Code of Practice

[Draft for consultation]



Intelligence services' use of third party bulk personal datasets

Presented to Parliament
by the Home Secretary
by Command of Her Majesty

[Autumn 2024]

CM XXXX

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

Any enquiries regarding this publication should be sent to us at [insert contact details].

ISBN XXX-X-XXXX-XXXX-X

XXXXXXXXXXXXX MM/YY

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of
the Controller of Her Majesty’s Stationery Office

Contents

1. Introduction

1.1. This code of practice relates to the exercise of functions conferred by virtue of Part 7B of the Investigatory Powers Act 2016 (“the Act”) as inserted by section 5 of the Investigatory Powers (Amendment) Act 2024. It should be read alongside Part 7B of the Act and the explanatory notes. It provides guidance on the procedures that must be followed before third party bulk personal datasets (3PD) can be accessed 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 may 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 an 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 examine personal information about a person by accessing third party bulk personal datasets. Other rights may also be engaged, such as the right to freedom of expression (Article 10).

1.6. Persons with the ability to access and examine, in situ, bulk personal datasets held by third parties 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 as appropriate.

2. Scope and definitions

2.1. The Act defines a bulk personal dataset (BPD) as a set of information that 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[1].

2.2. Part 7 and Part 7A of the Act make provision for the retention of BPDs by an intelligence service where the BPD is held electronically for analysis in the exercise of the service's functions.

2.3. Part 7B is concerned with circumstances in which a BPD is not retained by an intelligence service but is instead retained by a third party. It provides a statutory framework by means of which an intelligence service can examine a third party BPD (3PD) in situ, rather than obtaining and retaining the BPD itself.

2.3.1. Part 7B applies where an intelligence service has relevant access to a BPD that is held electronically by a third party and, after an initial inspection of the contents, the intelligence service examines the BPD electronically.

2.3.2. An intelligence service will have '**relevant access**' where they have directly arranged with the third party to have electronic access that is not generally available to others. This access will be in situ wherever the BPD is held by the third party, it will not be obtained and retained by the intelligence service.

2.3.3. A '**third party**' is a person other than an intelligence service[2]. This may include individuals, companies, government departments or other public authorities.

2.4. To fall within Part 7B, the intelligence service's electronic access to the 3PD must be as a result of a direct arrangement between them and the third party that holds the data.

2.4.1. To meet the definition of 'relevant access', the relevant electronic access to the data must be by an intelligence service. A member of an intelligence service accessing the data using the third party's system would only constitute access by the intelligence service where that member is acting in the course of their functions as a member of that service.

1 See section 199 in relation to Part 7 and s226E in relation to Part 7B.

2 See section 226E(1)(a).

2.4.2. Part 7B does not apply in situations such as where an employee of a third party examines the third party's data and reports back to the intelligence service. This would not be electronic access by an intelligence service.

2.5. When considering whether Part 7B applies to a particular set of information, the intelligence service must assess whether the type and extent of the access available is 'generally available' (whether on a commercial basis or otherwise)[3].

2.6. Accesses will be considered on a case-by-case basis. Examples of accesses that would be considered generally available include accesses that are widely available online, whether for free or upon payment of a charge, and accesses that are available to commercial customers.

2.7. Examples of access that is likely to be considered generally available include but are not limited to:

- access to an online encyclopaedia;
- access by subscription to an online newspaper (including where credentials may be needed to access an account);
- access to datasets that are made available for public searching (e.g. of company records);
- access to public phone or other directories;
- access to services that provide a general user with the ability to search across academic literature.

2.8. Part 7B will not apply where access is considered to be generally available.

2.9. Access will not be considered generally available where it is made available only to a particular group of individuals or organisations that fulfil a specific and limited set of qualifying criteria. For example, a particular access might only be available to public authorities, or to law enforcement agencies and intelligence services, or to bodies concerned with the protection of national security. Access to such datasets would be a relevant access for the purposes of section 226E.

2.10. Even where an intelligence service is able to examine in situ a set of information that is widely available, access may not be considered generally available if the nature of the intelligence service's access is broader than that which other users of the set enjoy. For example, the intelligence service might be able to query additional data fields that other users or customers cannot.

2.11. Examples of accesses that would not be generally available may include:

3 See section 226E(2)(b).

- access to data held by a UK government department which is not available to the public and that would constitute a BPD if retained by an intelligence service. For example, an intelligence service may access HMG-held immigration-related datasets to conduct checks to ensure those entering the UK do not pose a risk to national security.

- where a commercial company provides privileged access to an intelligence agency so additional data is made available to that agency over and above that which could be purchased by another client.

2.12. As set out in paragraph 2.3.3, a 'third party' is a person other than a UK intelligence service (Security Service, Secret Intelligence Service and Government Communications Head Quarters). This may include domestic or international individuals, companies, government departments, other public authorities. Therefore, Part 7B of the Act does not cover: any activity which may involve an intelligence service or any member of an intelligence service accessing data sets held by another UK intelligence service.

Initial Inspection

2.13. Considerable preliminary work may be needed on the part of the intelligence service and the third party on the relationship, before a 3PD access can be successfully established, and the 3PD is able to be examined for the purpose of the exercise of the intelligence service's functions.

2.14. Part 7B of the Act recognises this and allows an intelligence service to carry out an initial inspection of a 3PD before deciding whether to make an application to the Secretary of State for a 3PD warrant to authorise the examination of the 3PD for the purpose of the exercise of their statutory functions. Part 7B of the Act does not impose a timeframe for this initial inspection. The timeframe within which the initial inspection can take place will vary on a case-by-case basis and depend on a number of factors, including the matters set out at paragraph 2.15.

2.15. This initial inspection is likely to be necessary for a number of reasons, which may include:

- To assess the value of the data being made available.

- To assess whether the dataset constitutes a 3PD.

- To assess whether it is necessary and proportionate to seek access to the data.

- To establish practical steps for enabling access e.g., engineering and system access

- To establish the operational safety of access.

- To build a relationship with the third party supplier of the data and establish the nature of the access that will be required.

2.16. The initial inspection should be carried out by the minimum number of people necessary in order to do what is required, which will be assessed on a case-by-case basis.

2.17. As part of the initial assessment of value, it may be necessary to run data outputs from the 3PD under inspection through separate systems controlled by the intelligence service, for the sole purpose of assessing the potential value of the dataset. This may allow a fuller assessment of the necessity and proportionality of access to data to be made and inform the decision as to whether to seek a 3PD warrant.

2.18. The initial inspection may require that data in a possible 3PD is read, looked at or listened to by the intelligence service in order to establish the nature and value of the data and whether it will be necessary and proportionate to pursue an application to examine the data under Part 7B and within the meaning in section 226E.

2.19. The intelligence service may not examine the data further for operational or investigation reasons unless authorised by a warrant. The initial inspection must, therefore, relate to the viability and nature of the access to, and examination of, the 3PD."

2.20. If, after the initial inspection, the intelligence service assesses that examining the dataset falls within Part 7B, and that it would be necessary and proportionate to examine the 3PD in pursuit of its statutory functions, they should apply for a 3PD warrant.

2.21. If, after the initial inspection, the intelligence service assesses that it would not be necessary and proportionate to examine the 3PD, the 3PD should not be further accessed.

3. 3PD warrant applications

3.1. An application for a 3PD warrant is made to the Secretary of State. The requirements set out in Part 7B of the Act only relate to the intelligence services. An application for a 3PD 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).

3.2. All 3PD warrants are issued by the Secretary of State. No 3PD warrant may be issued unless and until the decision to do so has been approved by a Judicial Commissioner (see paragraph 4.14. and subsequent paragraphs). A Judicial Commissioner will have access to the same application for a warrant as the Secretary of State.

3.3. The only exception to this is a case where the Secretary of State considers that there is an urgent need to issue a warrant (see paragraph 4.19. 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 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 3PD warrant is issued, it is addressed to the person who submitted the application (or on whose behalf it was submitted).

3.4. Prior to submission, each application should be subject to a review within the intelligence service making the application. In conducting this review, the intelligence service must satisfy itself that:

- the application is necessary for one or more of the statutory purposes specified in section 226G 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 interest of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security; and
- the application is proportionate to what is sought to be achieved; only as much information will be accessed 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.

3.5. When completing a warrant application, 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.

3.6. Section 226G(5) makes clear that the fact that the information that would be examined 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.

Making an application

3.7. When making an application for a 3PD warrant, the intelligence service may either:

- make a single application to examine a single dataset.
- make a single application to examine multiple datasets or types of dataset brought together in a single access. For example, an arrangement may be in place with a third party that performs a service which brings together datasets from multiple sources and makes these available to query as a single access.
- make a single application to cover multiple 3PD accesses where those accesses raise similar considerations. For example, if an intelligence service has access to multiple 3PDs that are similar in content and degree of intrusion they might choose to group such accesses into a single 3PD warrant application, so that the Secretary of State could consider the necessity and proportionality case for those accesses in the round. This could include accesses which were not available at the time of the issue of the warrant.

3.8. The application for a 3PD warrant must include a general description of the bulk personal dataset or datasets to which the application relates. The description will necessarily be general in nature because the intelligence service is not itself in possession of the dataset or datasets to which access is being sought, and, as a result, in some cases it will not have more than a general knowledge of the data contained therein.

3.9. Moreover, where an access is provided by a third party which aggregates multiple datasets, the intelligence service may not be aware when particular new datasets are added to that access, or when other datasets are removed. Section 226F(3) recognises this by making it clear that a 3PD warrant may authorise the examination of a bulk personal dataset:

A) ‘the content of which may vary from time to time, or

B) that does not exist at the time of the issue of the warrant.’

Provided the datasets raise the same considerations and meet the general description within the issued warrant application, a warrant can therefore authorise the examination of datasets that are continually updated and that did not exist at the time of the issue of the warrant. Where it becomes known that the nature of the data falls beyond the general description, refer to paragraph 4.34.

Statements to the Secretary of State

3.10. Section 226G(3) provides for a number of situations where an intelligence service must include a statement to the Secretary of State in the warrant application. These statements are intended to make the Secretary of State aware of particular sensitive issues, so that the Secretary of State can take these into account when deciding whether or not to issue the warrant. The three situations in which a statement is required are set out in section 226G(6). The intelligence service must include a statement to the Secretary of State where the intelligence service knows that:

- the dataset consists of, or includes protected data[4] (as defined in Section 203 of the Act) or health records[5] (see section 226G(7)),
- a substantial proportion of the dataset consists of sensitive personal data[6] ,or
- the nature of the dataset, or the circumstances in which it was created, is or are such that its examination by the intelligence service is likely to raise novel or contentious issues.

3.11. The statement should identify which of the three situations in section 226G(6) are met, and concisely set out the relevant information for the Secretary of State. For example, the intelligence service might set out why it knows that the dataset contains health records or set out the novel or contentious issue raised by examination of this dataset or datasets. The intelligence service should also concisely set out why it believes that the examination of the 3PD is nevertheless necessary and proportionate.

4 ‘Protected data’ is defined in section 203 of the Act.

5 ‘Health record’ is defined by section 206(6) of the Act 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.

6 ‘Sensitive personal data’ for the purposes of the Act is as defined in section 86(7)(a) to (e)of the Data Protection Act 2018 but includes data relating to deceased individuals. Any references to sensitive personal data within this Code of Practice should be interpreted accordingly.

4. Authorisation of 3PD warrants by a Secretary of State

4.1. The Secretary of State may only issue a warrant under section 226G if the Secretary of State considers the following tests are met:

- The warrant 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 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.
- The arrangements made by the intelligence service for examining the bulk personal dataset (or datasets) to which the application relates are satisfactory. (See chapter 5 and subsequent paragraphs.)
- Except where a warrant is issued in an urgent case, a Judicial Commissioner has approved the decision to issue the warrant. (See paragraph 4.19. and subsequent paragraphs.)

4.2. In the event the Secretary of State is not satisfied that the case for the warrant has been sufficiently made out, the Secretary of State may request additional information or decline to issue the warrant. Where the Secretary of State refuses to issue the warrant, he or she may instead invite the relevant intelligence service to submit a revised application with additional information included where necessary.

4.3. Section 2 of the Act requires the issuing authority to have regard to the following when issuing, renewing, 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

Necessity and Proportionality

4.4. Where examination of a 3PD involves an interference with an individual's rights under Article 8 (right to respect for private and family life) of the ECHR, this will only be justifiable if the interference is necessary and proportionate. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the statutory purposes set out in sections 226G(4) 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.

When will examining a 3PD be necessary?

4.5. 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 examination, the intelligence services and the Secretary of State must consider why examining the 3PD is necessary for the statutory purposes set out in section 204(3)(a) or section 205(6)(a).

When will examining a 3PD be proportionate?

4.6. The Secretary of State must believe that examination of the 3PD 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.

4.7. 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 examination of the 3PD. 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.

4.8. 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.

Statements to the Secretary of State

4.9. There are a number of situations, set out at paragraphs 3.10-3.11 above, where the intelligence service must include a statement on particular sensitive issues.

4.10. When such a statement is included, the Secretary of State must take it into consideration when deciding whether or not to issue the warrant.

Authorisation: senior officials

4.11. The Act permits that when it is not reasonably practicable for the Secretary of State to sign a 3PD 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 3PD 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.

4.12. 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 226GB will apply.

4.13. The Act does not mandate how the Judicial Commissioner must show or record his or her decision. An approval will be communicated by the Commissioner on a decision sheet which may include comments from the Judicial Commissioner.

Judicial Commissioner approval

4.14. Before a 3PD 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.

4.15. Section 226GA of the Act provides that, when deciding whether to approve the decision to issue a 3PD 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. 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).

4.16. 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.

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

- not issue the warrant; or
- refer the matter to the Investigatory Powers Commissioner for a review of the Judicial Commissioner's decision (unless the Investigatory Powers Commissioner has made the original decision).

4.18. 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

4.19. Part 7B of the Act makes provision (see sections 226GB) for cases in which a 3PD warrant is required urgently.

4.20. In addition to the tests sets out at paragraph 4.1 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 3PDs to identify the vessel to prevent the weapons reaching the terrorist.

4.21. 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 basis of a written record produced by the senior official, 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).

4.22. 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 twelve months, in the same way as non-urgent 3PD warrants.

4.23. 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 impose conditions as to the use of any data examined under urgent warrant and subsequently acquired by the intelligence service. 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 on conditions relating to examination.

Duration of 3PD warrants

4.24. The duration of a warrant (other than an urgent warrant) is twelve 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 twelve-month duration begins on the day following the day on which it would otherwise have ceased to have effect.

Renewal of 3PD warrants

4.25. 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 should contain an update of the matters outlined in paragraph 3.8.

4.26. In particular, if the applicant is aware that the nature of the data has changed or evolved since the application or last renewal, this should be set out. The applicant must explain why it continues to be necessary to access and examine the 3PD, and why this continues to be proportionate.

4.27. In deciding whether to renew a 3PD warrant, the Secretary of State must consider whether the examination continues to be necessary and proportionate for one or more of the statutory purposes (as set out in the first bullet-point in paragraph 4.1 above) on the warrant.

4.28. When considering whether to renew a 3PD warrant, the Secretary of State will have regard to the updated renewal application, which will include:

- a general description of the data covered by the warrant;
- a note of any significant changes to the data since the warrant was last granted;
- whether any sensitive personal data (defined by paragraph 3.10) is known to be contained in the dataset;
- the necessity and proportionality case for the exploitation of the data;
- evidence, where available, of the utility of the data.

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

Cancellation of 3PD warrants

4.30. The Secretary of State, or a senior official acting on his or her behalf, may cancel a 3PD warrant at any time (see section 226HB). Such persons must cancel a 3PD warrant if, at any time before its expiry date, he or she considers that:

- the warrant is no longer necessary for any of the purposes for which a warrant may be issued;
- the conduct is no longer proportionate to what is sought to be achieved;

4.31. The intelligence services will therefore need to keep their 3PD 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.

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

4.33. 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 3PD, in the future should it be considered necessary and proportionate to do so.

4.34. There is no warrant modification process outlined within the Act. When the intelligence service knows of a change to the 3PD access set out in the original warrant, the warrant application should be updated at renewal stage. If at any time the intelligence service becomes aware of a change to an access such that the description of the access in the warrant application no longer accurately reflects the data the intelligence service is able to examine, it should seek a new warrant For example, this might occur where a third party makes changes to an access such that the description of the access in the warrant application no longer accurately reflects the data the intelligence service is able to examine.

4.35. In some cases, examination of a 3PD after the issue of the relevant warrant may lead the intelligence service to conclude that the nature of the data is such that section 226G(6) applies, when that may not have been stated in the relevant warrant application. In such a case, the intelligence service should provide a statement to the Secretary of State that they now know that section 226G(6) applies to 3PD to which the warrant relates.

Non-renewal or cancellation of 3PD warrants

4.36. Section 226HC provides for the situation where a 3PD warrant is not renewed or is cancelled.

4.37. Once a 3PD warrant has been cancelled, or the Secretary of State has declined to renew at 3PD warrant, no further examination of that 3PD may be carried out and the access to the 3PD must cease as soon as is reasonably practicable.

5. Safeguards

5.1. This chapter sets out the safeguards which each intelligence service should put in place in relation to access to and examination of 3PDs. The Secretary of State may only issue a 3PD warrant if s/he considers that the arrangements made for examining the bulk personal dataset (or datasets) to which the application relates are satisfactory (as set out in section 226G(4)(c)). The Secretary of State must also ensure that arrangements are in force to secure that any examination of data under a 3PD warrant is necessary and proportionate in all the circumstances (see section 226IA(1)).

5.2. The safeguards include the requirement for the examination of a 3PD 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 objectives in a less intrusive way; and the requirement for Secretary of State and Judicial Commissioner approval for 3PD warrants.

Examination

5.3. In relation to examination of information held in a 3PD, each intelligence service should have in place the following measures:

- Access to and examination of the information contained within the 3PD should be strictly limited to those with an appropriate business requirement to use that data;
- Individuals may only access information within a 3PD if examination of the 3PD is necessary for one or more of the relevant statutory purposes specified in the Act;
- If individuals access information within a 3PD with a view to subsequent disclosure of that information, in addition to satisfying the condition in the above bullet they may only 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);
- Before accessing or disclosing information, individuals must also consider whether to do so would be proportionate. 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 as appropriate;

- 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 3PD warrant can be issued.

Information reasonably available to the intelligence service

5.4. Under section 226IA(1), the Secretary of State must ensure that arrangements are in force for securing that any examination of data contained in a 3PD is necessary and proportionate in all the circumstances.

5.5. This requirement is subject to subsection (2), which sets out that, when considering the arrangements that are in force to secure that any examination of a 3PD is necessary and proportionate, the Secretary of State must in particular have regard to the information that is reasonably available to the intelligence services in relation to the examination of such data.

5.6. Information relating to examination of a 3PD is, in effect, a record or records of an intelligence service's activity with a particular dataset. This might include, for example (where feasible), records of searches or queries that an intelligence service makes. As 3PDs are not owned, stored or otherwise controlled by the intelligence service, the nature of the data, and how that data is accessed by the intelligence service, will vary significantly between different 3PDs and different third parties. It follows that the information relating to examination will also vary. For certain methods of accessing 3PDs, there may be clear technical limits on what information relating to examination is available.

5.7. Moreover, subsection 2 states that the Secretary of State must have regard to the information relating to examination that is 'reasonably available' to the intelligence service. There may be situations where certain forms of information relating to examination are technically, but not reasonably, available to the intelligence service. For example, detailed information relating to examination might only be available by directing the third party's attention towards intelligence service activity, which might not be desirable for reasons of operational security. Alternatively, collecting certain forms of information relating to examination might incur significant engineering cost. In both these examples, the information in question might be technically, but not reasonably, available to the intelligence service.

5.8. Understanding what information relating to examination is reasonably available to the intelligence service will require a case-by-case judgment to be made. This is particularly important because the nature of this information has implications for the examination safeguards that are applied to particular 3PD accesses. For example, if the reasonably available information includes logs of searches conducted, then it may be practicable and appropriate to require a periodic audit of examination conducted via that method of access. However, this should be considered on a case-by-case basis. The information relating to examination that is reasonably available to the intelligence service will vary between different methods of accessing 3PDs.

5.9. For each access or method of access, the intelligence service must judge what information is reasonably available and assess the appropriate measures to implement to ensure that examination is necessary and proportionate in all the circumstances. This should include consideration of whether or not it is practicable to implement an audit capability. The intelligence service must be able to demonstrate these measures to the IPC as required.

5.10. Any serious deficiencies in these safeguards must be brought to the attention of senior management and any breaches of safeguards must be reported to the Investigatory Powers Commissioner.

Documentation and inspection

5.11. For each method of accessing a 3PD or 3PDs, the intelligence service should consider, what information relating to examination is reasonably available. It should then consider and be able to demonstrate for the purpose of subsequent inspection, the package of safeguards that will be applied to that method of access. This will allow the intelligence service to demonstrate how it will ensure that examination of data under that method of access is necessary and proportionate in all the circumstances, as required by the relevant 3PD warrant(s). These arrangements, and any relevant documentation will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

Personnel Security

5.12. All persons within the intelligence services who may have access to 3PDs 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.

Confidential Information relating to members of sensitive professions

5.13. Most 3PDs are unlikely to contain confidential information relating to the sensitive professions. A 'sensitive profession' for these purposes includes lawyers, 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, and the Northern Ireland Assembly (see paragraph 5.22)).

5.14. Information relating to a member of a sensitive profession is unlikely, in and of itself, to be 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.

5.15. There are two scenarios in which the examination of a 3PD could give rise to the need for additional protection for confidential information relating to members of sensitive professions.

5.16. First, it is possible that a 3PD 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.

5.17. Secondly, there is a small possibility that examination of data in 3PDs 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 below must be applied.

5.18. The intelligence services should ensure that, before intelligence service staff use a 3PD specifically with the intention of searching for 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 alongside additional requirements laid out in Chapter 5. Sections 226IB and 226IC make provision for additional safeguards that apply where examination of the 3PD is intended or likely to identify items subject to legal privilege.

Additional examination safeguards for confidential information relating to sensitive professions

5.19. The intelligence services should ensure that, before intelligence service staff use a 3PD 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 5.13 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, reasonable steps should be taken to mark the disseminated information as confidential.

5.20. 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 3PD 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.

5.21. 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.

Examination relating to a member of a relevant legislature and constituency business

5.22. Where:

- an intelligence service wishes to examine a 3PD with the purpose of examining protected data relating to a member of a relevant legislature; and
- the intelligence service must obtain the prior written approval of the Secretary of State, the Judicial Commissioner and the Prime Minister before such protected data is selected for examination; the intelligence service must have obtained the prior approval of the Prime Minister.

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

5.24. Where the intention is to examine 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, or 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.

5.25. 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.

5.26. Any case where constituency business content is intentionally examined, and subsequently acquired and retained, should be recorded and made available to the Investigatory Powers Commissioner as soon as reasonably practicable or on the basis of agreement, with the Commissioner. Any content which has been retained should be made available to the Investigatory Powers Commissioner on request.

Material subject to legal privilege

5.27. 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. The privilege may also apply in relation to communications not involving a lawyer, where the communication involves a repetition of legal advice in circumstances in which the quality of confidentiality has been preserved.

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

5.29. 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.

5.30. 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 3PDs (whether deliberately or otherwise) is therefore subject to the additional safeguards set out in paragraph 5.19 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.

5.31. Examination of legally privileged material fields for examination. These paragraphs apply where an intelligence service wishes to search a 3PD and:

- the purpose, or one of the purposes of the search, is to examine protected data subject to legal privilege, or
- the use of the relevant search criteria is likely to identify such data.

5.32. Where these paragraphs apply (and without prejudice to chapter 3 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).

5.33. 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 and proportionate 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 examined 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.

5.34. 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 226IB include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege, and
- where the first bullet of paragraph 5.31 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 and to meet statutory functions. 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 examining the information.

5.35. 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 5.51.

Handling, retention and deletion

5.36. Officials who examine protected data contained in 3PDs should be alert to any data which may be subject to legal privilege.

5.37. 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 3PDs 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 3PD in question.

5.38. 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. The Investigatory Powers Commissioner should be informed as soon as practicable after retaining the item. The Investigatory Powers Commissioner will consider whether the item should be destroyed and if not, whether any

conditions should be applied on the retention. 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.

5.39. Where it is discovered that legally privileged protected data have been obtained inadvertently, an assessment must be made of whether it is necessary and proportionate to retain them must take place as soon as practicable. If it is assessed that the retention is not necessary and proportionate, the protected data should be marked for destruction, access prohibited and securely destroyed as soon as possible.

Dissemination of legally privileged material

5.40. 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.

5.41. 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.

5.42. 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

5.43. Where an item identified as subject to legal privilege following its examination is subsequently acquired and retained by the intelligence service, the relevant intelligence service must inform the Investigatory Powers Commissioner as soon as is reasonably practicable as per section 226IC(2). An approval is required from the Commissioner who will either impose conditions on the use of the retention or direct that the item is destroyed. 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

5.44. 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 in accordance with Article 10 ECHR.

5.45. 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.

5.46. 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.

5.47. 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).

5.48. 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.

5.49. 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.

5.50. 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.

5.51. 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.

5.52. Confidential journalistic protected data which have been identified as such, and data which identifies a source of journalistic information, should be examined only where it is necessary and proportionate to do so. There must be adequate information management systems in place to ensure that examination remains necessary and proportionate.

5.53. 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.

5.54. Where an item identified as confidential journalistic protected data following its examination is subsequently acquired and retained, the relevant intelligence service must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any data should be made available to the Investigatory Powers Commissioner on request.

Offence of breaching examination safeguards

5.55. Data contained within a 3PD may only be examined subject to the safeguards in sections 226IA of the Act. Section 226ID 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 examination is not necessary and proportionate.

Handling of material acquired by examining a 3PD

5.56. If data is retained as a result of the examination of, or after an initial inspection of a 3PD, such data will be treated in accordance with that intelligence service's existing handling arrangements, or other relevant policies, including retaining data only as long as it is necessary and proportionate to do so.

5.57. If, in the course of examining a 3PD, the intelligence service obtains, and subsequently wishes to retain, data that itself constitutes a BPD, the intelligence service would need to apply for a BPD warrant to retain or retain and examine that BPD under Part 7 or Part 7A IPA as appropriate.

6. Record-keeping and error reporting

6.1. 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 3PD warrants and all applications made for the renewal of such warrants;
- all 3PD warrant instruments, and renewal instruments; and
- where any application is refused, the grounds for refusal as given by the Secretary of State.

6.2. 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 3PD warrant;
- written records, including contemporaneous notes, of requests for urgent authorisations of warrants
- 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.

6.3. 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 3PD warrants submitted;
- the number of applications for 3PD warrants refused by the Secretary of State;
- the number of decisions to issue 3PD warrants not approved by a Judicial Commissioner;

- the number of 3PD warrants issued by the Secretary of State and approved by a Judicial Commissioner;
- the number of times an urgent 3PD 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 3PD warrant has subsequently not been approved by a Judicial Commissioner;
- the number of renewals of 3PD warrants that were made;
- the number of 3PD warrants that were cancelled;
- the number of 3PD warrants extant at the end of the calendar year.

6.4. 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.

6.5. 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

6.6. This section provides information regarding errors. Proper application of the Investigatory Powers Act as amended by the Investigatory Powers (Amendment) Act 2024 and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, should reduce the scope for making errors.

6.7. 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.

6.8. 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.

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

- A 3PD has been examined without lawful authority;

- There has been a failure to adhere to the restrictions on the use or disclosure of material imposed by sections 226IA-226IC.

6.10. 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.

6.11. 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.

6.12. 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 Investigatory Powers Commissioner, the intelligence service responsible must also inform the Commissioner of when it was initially identified that an error may have taken place.

6.13. 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; any unintended collateral intrusion; any analysis or action taken; and a summary of the steps taken to prevent recurrence.

6.14. As set out at section 231 (9) of the Act, the Investigatory Powers 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.

6.15. This section of the code cannot provide an exhaustive list of possible errors that would fall within paragraph 6.9 above. However, examples could include:

- Examining a 3PD after the initial inspection has been completed without having a relevant 3PD warrant in place;
- Examining a 3PD for operational or investigative purposes without having a 3PD warrant in place;
- Continuing to examine a 3PD after the relevant 3PD warrant has been cancelled or has expired; or
- Conducting examination of a 3PD in breach of the requirement for additional safeguards for material subject to legal privilege.

6.16. Where an error occurs which is also considered to constitute an offence detailed in chapter 5.55 of this code, the provisions of this chapter must still be applied to the handling of the error.

Serious errors

6.17. Section 231 of the Act states that the Investigatory Powers 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 Investigatory Powers 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.

6.18. In deciding whether it is in the public interest for the person concerned to be informed of the error, the Investigatory Powers 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.

6.19. Before making his or her decision, the Investigatory Powers 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.

6.20. When informing a person of a serious error, the Investigatory Powers 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.

7. Oversight

7.1. The Investigatory Powers Act 2016 provides for an Investigatory Powers Commissioner ("the Commissioner"), and under the Investigatory Powers Act 2016 as amended by the Investigatory Powers (Amendment) Act 2024, the Commissioner's remit includes providing comprehensive oversight of the use of the powers contained within Part 7B 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 His 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.

7.2. 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.

7.3. The Commissioner will have unfettered access to all of the intelligence service's 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 His 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.

7.4. 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 6 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 or as an alternative to raising a

concern internally through a disclosure to IPCO, as enabled by the information gateway set out in section 237 of the IPA[7].

7.5. 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 6 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 8 for more information on how this can be done).

7.6. 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.

7.7. 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.

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

[7] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/2022-08-Disclosing-information-to-IPCO.pdf

8. Complaints

8.1. 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.

8.2. 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.

8.3. 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: www.ipt-uk.com.

8.4. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

8.5. 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.

XXX-X-XXXX-XXXX-X

XXXXXXXXXXXXX