Investigatory Powers (Amendment) Act 2024

2024 CHAPTER 9

An Act to amend the Investigatory Powers Act 2016; to make provision about information supplied by, or relating to, the Judicial Commissioners; and for connected purposes. [25th April 2024]

BE IT ENACTED by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1

BULK PERSONAL DATASETS

Low or no reasonable expectation of privacy

1 Requirement for authorisation

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 199 (bulk personal datasets: interpretation)—

(a) in subsection (1), in the words before paragraph (a), after "Part" insert "and Part 7A";

(b) in subsection (2), after "Part" insert "and Part 7A".

(3) In the italic heading before section 200, for "warrant" substitute "authorisation".

(4) In section 200 (requirement for authorisation by warrant: general)—

(a) in subsection (1)—

(i) the words "by a warrant under this Part" become paragraph (a);

(ii) after that paragraph insert ", or

(b) by an individual authorisation under Part 7A (low or no reasonable expectation of privacy) (see section 226B).";

(b) in subsection (2)—

(i) the words "by a warrant under this Part" become paragraph (a);

(ii) after that paragraph insert ", or

(b) by an individual authorisation under Part 7A.";

(c) in the heading, omit "by warrant".

(5) In section 201 (exceptions to section 200(1) and (2)), in subsection (3)—

(a) for "and 220(5)" substitute ", 220(5) and (6) and 226CC(3)";

(b) after "BPD warrants" insert "or authorisations under Part 7A".

(6) After section 201 insert—

"Restriction on use of class BPD warrants etc".

(7) In section 220 (initial examinations: time limits)—

(a) in subsection (2), for step 3 substitute—

"Step 3

If the head of the intelligence service, or a person acting on their behalf, decides to retain the set and hold it electronically for analysis as mentioned in step 2, as soon as reasonably practicable after making that decision—

(a) apply for a specific BPD warrant (unless the retention of the dataset is authorised by a class BPD warrant), or

(b) where the head of the intelligence service, or the person acting on their behalf, considers that section 226A applies to the dataset, decide to grant an individual authorisation under Part 7A.";

(b) after subsection (5) insert—

"(6) If the head of the intelligence service, or a person acting on their behalf, decides to grant an individual authorisation under Part 7A in accordance with step 3 (set out in subsection (2))—

(a) the intelligence service is not to be regarded as in breach of section 200(1) by virtue of retaining the bulk personal dataset during any period when a Judicial Commissioner is deciding whether to approve the decision to grant the authorisation (see section 226B(5)), and

(b) the intelligence service is not to be regarded as in breach of section 200(2) by virtue of examining the bulk personal dataset during that period if the examination is necessary in connection with obtaining the approval of a Judicial Commissioner."

(8) In section 225 (application of Part 7 to bulk personal datasets obtained under the Act)—

(a) in subsection (4)—

(i) the words "by a class BPD warrant or a specific BPD warrant under this Part" become paragraph (a);

(ii) after that paragraph insert ", or

(b) by an individual authorisation under Part 7A (low or no reasonable expectation of privacy).";

(b) in subsection (13)—

(i) the words from "apply" to the end become paragraph (a);

(ii) after that paragraph insert ", or

(b) decide to grant an individual authorisation under Part 7A."

2 Low or no reasonable expectation of privacy

After Part 7 of the Investigatory Powers Act 2016 insert—

"**PART 7A**

BULK PERSONAL DATASET AUTHORISATIONS

Low or no reasonable expectation of privacy

226A Bulk personal datasets: low or no reasonable expectation of privacy

(1) This section applies to a bulk personal dataset if the nature of the bulk personal dataset is such that the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to the data.

(2) In considering whether this section applies to a bulk personal dataset, regard must be had to all the circumstances, including in particular the factors in subsection (3).

(3) Those factors are—

(a) the nature of the data;

(b) the extent to which—

(i) the data has been made public by the individuals, or

(ii) the individuals have consented to the data being made public;

(c) if the data has been published, the extent to which it was published subject to editorial control or by a person acting in accordance with professional standards;

(d) if the data has been published or is otherwise in the public domain, the extent to which the data is widely known about;

(e) the extent to which the data has already been used in the public domain.

Issue of authorisations

226B Individual authorisation

(1) In this Part "an individual authorisation" is an authorisation that authorises an intelligence service to retain, or to retain and examine, any bulk personal dataset described in the authorisation.

(2) See section 200 (requirement for authorisation) for provision about when an individual authorisation under this Part is required.

(3) The head of an intelligence service, or a person acting on their behalf, may grant an individual authorisation where the conditions in subsections (4) and (5) are met.

This is subject to subsection (6).

(4) The condition in this subsection is that the person granting the authorisation considers that—

(a) section 226A applies to the bulk personal dataset described in the authorisation,

(b) the authorisation is necessary for the purpose of the exercise of any function of the intelligence service,

(c) the conduct being authorised is proportionate to what is sought to be achieved by the conduct, and

(d) there are for the time being in force arrangements made by the intelligence service, and approved by the Secretary of State, for storing bulk personal datasets to which section 226A applies and for protecting them from unauthorised disclosure.

(5) The condition in this subsection is that the decision to grant the authorisation has been approved by a Judicial Commissioner.

(6) The condition in subsection (5) does not apply where—

(a) the bulk personal dataset described in the individual authorisation falls within a category of bulk personal datasets authorised for the purposes of this Part by a category authorisation (see section 226BA), or

(b) the person granting the individual authorisation considers that there is an urgent need to grant the authorisation.

(7) But subsection (6)(a) does not prevent a person granting an individual authorisation from seeking the approval of a Judicial Commissioner in a case where subsection (6)(a) applies if the person considers that it would be appropriate to seek such approval.

(8) An individual authorisation relating to a bulk personal dataset ("dataset A") may also authorise the retention or examination of other bulk personal datasets ("replacement datasets") that do not exist at the time of the grant of the authorisation but may reasonably be regarded as replacements for dataset A.

226BA Category authorisation

(1) In this Part "a category authorisation" is an authorisation that authorises a category of bulk personal datasets described in the authorisation for the purposes of this Part.

(2) The head of an intelligence service, or a person acting on their behalf, may grant a category authorisation where—

(a) they consider that section 226A applies to any dataset that falls within the category of datasets described in the authorisation, and

(b) the decision to grant the authorisation has been approved by a Judicial Commissioner.

(3) A category authorisation may describe a category of bulk personal datasets by reference to (among other things) the use to which the datasets will be put.

226BB Approval of authorisations by Judicial Commissioners

(1) In deciding whether to approve a decision to grant an individual authorisation or a category authorisation, a Judicial Commissioner must review the conclusions of the person who granted the authorisation as to the following matters—

(a) in relation to an individual authorisation, whether section 226A applies to the bulk personal dataset described in the authorisation, and

(b) in relation to a category authorisation, whether section 226A applies to any dataset that falls within the category of datasets described in the authorisation.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to grant an individual authorisation or a category authorisation, the Judicial Commissioner must give the person who decided to grant the authorisation written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to grant an individual authorisation or a category authorisation, the head of the intelligence service, or a person acting on their behalf, may ask the Investigatory Powers Commissioner to decide whether to approve the decision to grant the authorisation.

226BC Approval of individual authorisations granted in urgent cases

(1) This section applies where—

(a) an individual authorisation is granted without the approval of a Judicial Commissioner, and

(b) the person who granted the authorisation considered that there was an urgent need to grant it.

(2) The person who granted the authorisation must inform a Judicial Commissioner that it has been granted.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to grant the authorisation, and

(b) notify the person who granted the authorisation of the Judicial Commissioner's decision.

The "relevant period" means the period ending with the third working day after the day on which the authorisation was granted.

(4) Subsections (5) to (7) apply if a Judicial Commissioner refuses to approve the decision to grant an individual authorisation.

(5) The authorisation—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 226BB(4) does not apply in relation to the refusal to approve the decision.

(6) The head of the intelligence service must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the authorisation stops as soon as possible.

(7) Section 220 (Part 7 initial examinations: time limits) applies in relation to the bulk personal dataset described in the authorisation as if the intelligence service had obtained that dataset at the time when the person who granted the authorisation is notified that the Judicial Commissioner has refused to approve the decision to grant the authorisation.

(8) Nothing in subsection (5) or (6) affects the lawfulness of—

(a) anything done in reliance on the authorisation before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the authorisation when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

Duration, renewal and cancellation

226C Duration of authorisation

(1) An individual authorisation or a category authorisation ceases to have effect at the end of the relevant period unless—

(a) it is renewed before the end of that period (see section 226CA), or

(b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 226BC, 226CB, and 226CD).

(2) In this section the "relevant period"—

(a) in the case of an urgent individual authorisation, means the period ending with the fifth working day after the day on which the authorisation was granted;

(b) in any other case, means the period of 12 months beginning with—

(i) the day on which the authorisation was granted, or

(ii) in the case of an authorisation that has been renewed, the day after the day at the end of which the authorisation would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a), an individual authorisation is an "urgent individual authorisation" if—

(a) the authorisation was granted without the approval of a Judicial Commissioner, and

(b) the person who granted the authorisation considered that there was an urgent need to grant it.

226CA Renewal of authorisation

(1) If the renewal conditions are met for an individual authorisation or a category authorisation, the head of an intelligence service, or a person acting on their behalf, may, at any time during the renewal period, renew the authorisation.

(2) The renewal conditions for an individual authorisation are that—

(a) the person renewing the authorisation considers that—

(i) section 226A continues to apply to the bulk personal dataset described in the authorisation,

(ii) the authorisation continues to be necessary for the purpose of the exercise of any function of the intelligence service,

(iii) the conduct being authorised continues to be proportionate to what is sought to be achieved by the conduct, and

(iv) there are for the time being in force arrangements made by the intelligence service, and approved by the Secretary of State, for storing bulk personal datasets to which section 226A applies and for protecting them from unauthorised disclosure, and

(b) the decision to renew the authorisation has been approved by a Judicial Commissioner.

(3) But the condition in subsection (2)(b) does not apply where the bulk personal dataset described in the individual authorisation falls within a category of bulk personal datasets authorised for the purposes of this Part by a category authorisation.

(4) The renewal conditions for a category authorisation are that—

(a) the person renewing the authorisation considers that section 226A continues to apply to any dataset that falls within the category of datasets described in the authorisation, and

(b) the decision to renew the authorisation has been approved by a Judicial Commissioner.

(5) In this section the "renewal period" means—

(a) in the case of an urgent individual authorisation which has not been renewed, the relevant period;

(b) in the case of an individual authorisation to which section 226CD (non-renewal or cancellation of category authorisation) applies, the period of three months ending with the day at the end of which the authorisation would otherwise cease to have effect;

(c) in any other case, the period of 30 days ending with the day at the end of which the authorisation would otherwise cease to have effect.

(6) Section 226BB (approval of authorisations by Judicial Commissioner) applies in relation to a decision to renew an authorisation under this section as it applies in relation to a decision to grant an authorisation under this Part.

(7) In this section—

"the relevant period" has the same meaning as in section 226C;

"urgent individual authorisation" is to be read in accordance with subsection (3) of that section.

226CB Cancellation of authorisation

(1) The head of an intelligence service, or a person acting on their behalf, may, at any time, cancel an individual authorisation or a category authorisation.

(2) If the head of an intelligence service, or a person acting on their behalf, considers that any of the cancellation conditions are met in relation to an individual authorisation, or that the cancellation condition is met in relation to a category authorisation, they must cancel the authorisation.

(3) The cancellation conditions for an individual authorisation are—

(a) that section 226A no longer applies to the dataset described in the authorisation;

(b) that the authorisation is no longer necessary for the purpose of the exercise of any function of the intelligence service;

(c) that the conduct authorised by the authorisation is no longer proportionate to what is sought to be achieved by the conduct;

(d) that there are no longer in force arrangements made by the intelligence service, and approved by the Secretary of State, for storing bulk personal datasets to which section 226A applies and for protecting them from unauthorised disclosure.

(4) The cancellation condition for a category authorisation is that section 226A no longer applies to any dataset that falls within the category of datasets described in the authorisation.

226CC Non-renewal or cancellation of individual authorisation

(1) This section applies where an individual authorisation ceases to have effect because it expires without having been renewed or because it is cancelled.

(2) The head of the intelligence service, or a person acting on their behalf, may, before the end of the period of 5 working days beginning with the day on which the authorisation ceases to have effect, decide to grant a new individual authorisation (see section 226B) to retain, or to retain and examine, any material retained by the intelligence service in reliance on the authorisation which has ceased to have effect.

(3) Where an individual authorisation ceases to have effect because it expires without having been renewed or because it is cancelled, an intelligence service is not to be regarded as in breach of section 200(1) or (2) by virtue of its retention or examination of any material to which the authorisation related during the following periods—

(a) the period of 5 working days beginning with the day on which the authorisation ceases to have effect;

(b) if the head of the intelligence service, or a person acting on their behalf, decides to grant a new individual authorisation as mentioned in

subsection (2), any period when a Judicial Commissioner is deciding whether to approve the decision.

226CD Non-renewal or cancellation of category authorisation

(1) This section applies where—

(a) a category authorisation ceases to have effect because it expires without having been renewed or because it is cancelled, and

(b) an individual authorisation describing a bulk personal dataset that falls within the category of datasets described in the category authorisation has been granted without the approval of a Judicial Commissioner in accordance with section 226B(6)(a).

(2) The individual authorisation ceases to have effect at the end of the relevant period unless—

(a) it is renewed before the end of that period, or

(b) it is cancelled or otherwise ceases to have effect before the end of that period.

(3) In this section the "relevant period" means the period of three months beginning with the day after the day at the end of which the category authorisation ceased to have effect.

Further and supplementary provision

226D Section 226A ceasing to apply to part of bulk personal dataset

(1) Subsections (2) to (4) apply where—

(a) an individual authorisation is granted under this Part in relation to any bulk personal dataset, and

(b) in the course of examining the dataset in accordance with the authorisation, the head of the intelligence service, or a person acting on their behalf, believes that section 226A does not apply, or no longer applies, to part of the dataset.

(2) The head of the intelligence service must, so far as is reasonably practicable, secure that anything in the process of being done in relation to that part of the bulk personal dataset in reliance on the authorisation stops as soon as possible.

(3) Section 220 (Part 7 initial examinations: time limits) applies in relation to that part of the bulk personal dataset as if the intelligence service had obtained that part of the dataset at the time when the head of the intelligence service, or the person acting on their behalf, first formed the beliefs mentioned in subsection (1)(b).

(4) The individual authorisation in relation to that part of the bulk personal dataset is to be treated as if it had been cancelled under section 226CB at that time.

(5) Nothing in this section affects the lawfulness of—

(a) anything done in reliance on the authorisation before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the authorisation when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

226DA Annual report

(1) The head of each intelligence service must provide an annual report to the Secretary of State about the bulk personal datasets that were authorised under this Part to be retained, or retained and examined, by the intelligence service during the period to which the report relates.

(2) The first report must relate to a period of at least one year and no more than two years, beginning with the day on which this Part comes fully into force.

(3) Subsequent reports must relate to a period of no more than one year, beginning with the end of the period to which the previous report related.

(4) Each report must be provided to the Secretary of State as soon as reasonably practicable after the end of the period to which the report relates.

226DB Report to Intelligence and Security Committee

(1) The Secretary of State must for each relevant period provide to the Intelligence and Security Committee of Parliament a report setting out information about category authorisations and renewals of category authorisations granted in that period.

(2) In subsection (1) "relevant period" means—

(a) a period of at least one year and no more than two years beginning with the date on which this Part comes fully into force, and

(b) subsequent periods of no more than one year, beginning with the end of the period to which the previous report related.

(3) Each report must be provided to the Committee as soon as reasonably practicable after the end of the period to which the report relates.

226DC Part 7A: interpretation

(1) In this Part—

"category authorisation" has the meaning given by section 226BA(1);

"individual authorisation" has the meaning given by section 226B(1).

(2) See also—

section 199 (bulk personal datasets: interpretation),

section 263 (general definitions),

section 265 (index of defined expressions).

(3) For the purposes of this Part, only a person holding office under the Crown may act on behalf of the head of an intelligence service."

Bulk personal dataset warrants

3 Duration of bulk personal dataset warrants

(1) In section 213 of the Investigatory Powers Act 2016 (duration of warrants), in subsection (2)(b), for "6 months" substitute "12 months".

(2) The amendment made by subsection (1) has effect only in relation to a warrant that is issued or renewed under Part 7 of that Act on or after the day on which this section comes into force.

(3) In subsection (2) "warrant" has the same meaning as in section 213(2)(b) of that Act.

4 Agency head functions

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 202 (restriction on use of class BPD warrants)—

(a) in subsections (1) and (2), after "head of the intelligence service" insert ", or a person acting on their behalf,";

(b) in subsection (3)—

(i) after "head of the intelligence service", in the first place it occurs, insert ", or a person acting on their behalf,";

(ii) omit "by the head of the intelligence service";

(c) after subsection (4) insert—

"(5) For the purposes of subsections (1), (2) and (3), only a person holding office under the Crown may act on behalf of the head of an intelligence service."

(3) In section 206 (additional safeguards for health records)—

(a) in subsections (4)(b) and (5)(a) and (b), after "head of the intelligence service" insert ", or a person acting on their behalf,";

(b) after subsection (7) insert—

"(8) For the purposes of subsections (4)(b) and (5), only a person holding office under the Crown may act on behalf of the head of an intelligence service."

(4) In section 219 (non-renewal or cancellation of BPD warrants)—

(a) in subsection (2), after "addressed" insert ", or a person acting on their behalf,";

(b) in the following provisions, after "the head of the intelligence service" insert ", or a person acting on their behalf,"—

(i) subsection (2)(b);

(ii) subsection (7), in both places it occurs;

(iii) subsection (8), in both places it occurs;

(c) after subsection (8) insert—

"(9) For the purposes of subsections (2), (7) and (8), only a person holding office under the Crown may act on behalf of the head of an intelligence service."

(5) In section 220 (initial examinations: time limits)—

(a) in the following provisions, after "head of the intelligence service" insert ", or a person acting on their behalf,"—

(i) subsection (1)(b);

(ii) subsection (2);

(iii) subsection (3);

(iv) subsection (5);

(b) after subsection (6) (inserted by section 1) insert—

"(7) For the purposes of this section, only a person holding office under the Crown may act on behalf of the head of an intelligence service."

(6) In section 225 (application of Part 7 to bulk personal datasets obtained under this Act)—

(a) in subsection (3), after "head of the intelligence service" insert ", or a person acting on their behalf";

(b) in subsection (13), after "head of an intelligence service" insert ", or a person acting on their behalf,";

(c) after subsection (14) insert—

"(15) For the purposes of subsections (3) and (13), only a person holding office under the Crown may act on behalf of the head of an intelligence service."

Third party bulk personal datasets

5 Third party bulk personal datasets

After Part 7A of the Investigatory Powers Act 2016 (as inserted by section 2) insert—

"**PART 7B**

THIRD PARTY BULK PERSONAL DATASETS

Interpretation

226E Third party bulk personal datasets: interpretation

(1) For the purposes of this Part, an intelligence service examines a third party bulk personal dataset if—

(a) the intelligence service has relevant access, whether on payment or otherwise, to a set of information that is held electronically by a person other than an intelligence service,

(b) the set includes personal data relating to a number of individuals,

(c) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions, and

(d) after any initial inspection of the contents (see section 226I), the intelligence service examines the set electronically (but does not obtain the set) for the purpose of the exercise of its functions.

(2) For the purposes of subsection (1)(a), an intelligence service has "relevant access" to a set of information that is held electronically by another person where—

(a) the access is made available to the intelligence service as a result of arrangements made directly between the intelligence service and that other person,

(b) the type and extent of the access available to the intelligence service is not generally available (whether on a commercial basis or otherwise), and

(c) the access is electronic.

Requirement for warrant

226F Requirement for authorisation by warrant

(1) An intelligence service may not exercise a power to examine a third party bulk personal dataset unless the examination of the dataset is authorised by a third party BPD warrant.

(2) A "third party BPD warrant" is a warrant issued under this Part authorising an intelligence service to examine any third party bulk personal dataset described in the warrant.

(3) A third party BPD 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.

226FA Exceptions to section 226F(1)

(1) Section 226F(1) does not apply to the exercise of a power of an intelligence service to examine a third party bulk personal dataset if the intelligence service examines the bulk personal dataset under any other warrant or authorisation issued or given under this Act.

(2) See section 226I(5) (initial inspection) for a further exception to 226F(1).

Issue of warrants

226G Application for third party BPD warrant

(1) The head of an intelligence service, or a person acting on their behalf, may apply to the Secretary of State for a third party BPD warrant.

(2) The application must include a general description of the bulk personal dataset (or datasets) to which the application relates.

(3) Where the person making the application knows that subsection (6) applies to any bulk personal dataset to which the application relates, the application must also include a statement to that effect.

(4) The Secretary of State may issue the warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security,

(ii) for the purposes of preventing or detecting serious crime, or

(iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,

(c) the Secretary of State considers that the arrangements made by the intelligence service for examining the bulk personal dataset (or datasets) to which the application relates are satisfactory, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(5) The fact that a third party BPD warrant would authorise the examination of bulk personal datasets relating to activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (4)(a).

(6) This subsection applies to a bulk personal dataset if—

(a) the dataset consists of, or includes, protected data or health records,

(b) a substantial proportion of the dataset consists of sensitive personal data, or

(c) 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.

(7) In this section—

"health record" means a record, or a copy of a record which—

(a) consists of information relating to the physical or mental health or condition 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 person (mentioned in section 226E(1)(a)) who holds the dataset, from a health professional or a health service body or from a person acting on behalf of a health professional or a health service body in relation to the record or the copy;

"sensitive personal data" has the meaning given by section 202(4).

(8) In subsection (7), "health professional" and "health service body" have the meaning given by section 206(7).

(9) An application for a third party BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

226GA Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a third party BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary on grounds falling within section 226G(4)(a), and

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a third party BPD warrant, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a third party BPD warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

226GB Approval of third party BPD warrants issued in urgent cases

(1) This section applies where—

(a) a third party BPD warrant is issued without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to issue it.

(2) The Secretary of State must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

The "relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) Subsections (5) and (6) apply if a Judicial Commissioner refuses to approve the decision to issue a third party BPD warrant.

(5) The warrant—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 226GA(4) does not apply in relation to the refusal to approve the decision.

(6) The head of the intelligence service to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant stops as soon as possible.

(7) Nothing in subsection (5) or (6) affects the lawfulness of—

(a) anything done in reliance on the warrant before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

226GC Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a third party BPD warrant must be taken personally by the Secretary of State.

(2) Before a third party BPD warrant is issued, it must be signed by the Secretary of State.

(3) But if it is not reasonably practicable for a third party BPD warrant to be signed by the Secretary of State, it may be signed by a senior official designated by the Secretary of State for that purpose.

(4) In such a case, the warrant must contain a statement that—

(a) it is not reasonably practicable for the warrant to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the issue of the warrant.

226GD Requirements that must be met by warrants

A third party BPD warrant must—

(a) be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made, and

(b) include a general description of the bulk personal dataset (or datasets) to which the warrant relates.

Duration, renewal and cancellation

226H Duration of warrants

(1) A third party BPD warrant ceases to have effect at the end of the relevant period unless—

(a) it is renewed before the end of that period (see section 226HA), or

(b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 226GB and 226HB).

(2) In this section "the relevant period"—

(a) in the case of an urgent third party BPD warrant, means the period ending with the fifth working day after the day on which the warrant was issued, and

(b) in any other case, means the period of 12 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of this section, a third party BPD warrant is an "urgent third party BPD warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to issue it.

226HA Renewal of warrants

(1) If the renewal conditions are met, a third party BPD warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary on grounds falling within section 226G(4)(a),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by the conduct, and

(c) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) In this section the "renewal period" means—

(a) in the case of an urgent third party BPD warrant which has not been renewed, the relevant period;

(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a third party BPD warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 226GA (approval of warrants by Judicial Commissioner) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

(6) In this section—

"the relevant period" has the same meaning as in section 226H;

"urgent third party BPD warrant" is to be read in accordance with subsection (3) of that section.

226HB Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a third party BPD warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a third party BPD warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary on any grounds falling within section 226G(4)(a);

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct.

226HC Non-renewal or cancellation of third party BPD warrant

(1) This section applies where a third party BPD warrant ceases to have effect because it expires without having been renewed or because it is cancelled.

(2) The head of the intelligence service to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant stops as soon as possible.

(3) Nothing in this section affects the lawfulness of—

(a) anything done in reliance on the warrant before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

Further and supplementary provision

226I Initial inspection

(1) This section applies where—

(a) an intelligence service has relevant access, whether on payment or otherwise, to a set of information that is held electronically by a person other than an intelligence service,

(b) the intelligence service is considering examining the set of information electronically for the purpose of the exercise of its functions,

(c) the examination would be otherwise than in the exercise of a power conferred by a warrant or other authorisation issued or given under this Act, and

(d) the head of the intelligence service, or a person acting on their behalf, believes that—

(i) the set includes, or may include, personal data relating to a number of individuals, and

(ii) the nature of the set is, or may be, such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions.

(2) The head of the intelligence service, or a person acting on their behalf, may carry out an initial inspection of the contents of the set for the purpose of deciding whether, if the intelligence service were to examine it after that initial inspection—

(a) the intelligence service would be examining a third party bulk personal dataset (see section 226E), and

(b) such examination would be necessary and proportionate in all the circumstances.

(3) Subsection (4) applies if, after the initial inspection is carried out, the head of the intelligence service, or a person acting on their behalf, decides that—

(a) the intelligence service would be examining a third party bulk personal dataset (as mentioned in subsection (2)(a)), and

(b) such examination would be necessary and proportionate in all the circumstances.

(4) The head of the intelligence service, or a person acting on their behalf, must—

(a) decide whether to examine the third party bulk personal dataset, and

(b) if they decide to do so, apply for a third party BPD warrant.

(5) If the head of the intelligence service, or a person acting on their behalf, applies for such a third party BPD warrant, the intelligence service is not to be regarded as in breach of section 226F(1) by virtue of examining the bulk personal dataset if the examination is necessary for the purposes of the making of the application for the warrant.

(6) For the purposes of subsection (1)(a), "relevant access" is to be read in accordance with section 226E(2).

(7) For the purposes of this section, only a person holding office under the Crown may act on behalf of the head of an intelligence service.

226IA Safeguards relating to examination of third party bulk personal datasets

(1) The Secretary of State must ensure, in relation to every third party BPD warrant which authorises the examination of a bulk personal dataset, that arrangements are in force for securing that any examination of data contained in the dataset is necessary and proportionate in all the circumstances.

(2) In doing so, 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.

226IB Additional safeguards for items subject to legal privilege: examination

(1) Subsections (2) and (3) apply if, in a case where protected data contained in a third party bulk personal dataset is to be examined in reliance on a third party BPD warrant—

(a) the purpose, or one of the purposes, of using the criteria to be used for the examination of the data ("the relevant criteria") is to identify any items subject to legal privilege, or

(b) the use of the relevant criteria is likely to identify such items.

(2) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the examination, the data may be examined using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(3) In any other case, the data may be examined using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(4) The Secretary of State may give approval for the purposes of subsection (2) only with the approval of a Judicial Commissioner.

(5) Approval may be given under subsection (2) or (3) only if, where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official considers that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.

(6) In deciding whether to give an approval under subsection (2) or (3) in a case where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official must have regard to the public interest in the confidentiality of items subject to legal privilege.

(7) For the purposes of subsection (5), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the examination of the data outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(8) In deciding whether to give approval for the purposes of subsection (4), the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(9) Subsections (10) and (11) apply if, in a case where protected data contained in a third party bulk personal dataset is to be examined in reliance on a third party BPD warrant—

(a) the purpose, or one of the purposes, of using the criteria to be used for the examination of the data ("the relevant criteria") is to identify data that, if the data or any underlying material were not created or held with the intention of furthering a criminal purpose, would be an item subject to legal privilege, and

(b) the person to whom the warrant is addressed considers that the data ("the targeted data") or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(10) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the examination, the data may be examined using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(11) In any other case, the data may be examined using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(12) Approval may be given under subsection (10) or (11) only if the Secretary of State or (as the case may be) the senior official considers that the targeted data or the underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(13) In this section "underlying material", in relation to data contained in a third party bulk personal dataset that is to be examined in reliance on a third party BPD warrant, means any communications or other items of information from which the data was produced.

226IC Additional safeguards for items subject to legal privilege: retention following examination

(1) Subsection (2) applies where—

(a) an intelligence service examines a third party bulk personal dataset in reliance on a third party BPD warrant,

(b) as part of the examination, the intelligence service examines an item subject to legal privilege,

(c) the intelligence service retains the item, and

(d) the retention of the item may not be authorised by a warrant under Part 7 (bulk personal dataset warrants).

(2) The person to whom the third party BPD warrant (mentioned in subsection (1)(a)) is addressed must inform the Investigatory Powers Commissioner as soon as reasonably practicable after retaining the item.

(3) Unless the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(4) If the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (3)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(6) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(7) Each of the following is an "affected party" for the purposes of subsection (6)—

(a) the Secretary of State;

(b) the person to whom the third party BPD warrant is or was addressed.

226ID Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person examines, in reliance on a third party BPD warrant, any data contained in a third party bulk personal dataset,

(b) the person knows or believes that the examination of that data is in breach of the requirement specified in subsection (2), and

(c) the person deliberately examines that data in breach of that requirement.

(2) The requirement specified in this subsection is that any examination of the data is necessary and proportionate.

(3) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court, to a fine or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months, to a fine not exceeding the statutory maximum or to both;

(c) on summary conviction in Northern Ireland, to imprisonment for a term not exceeding 6 months, to a fine not exceeding the statutory maximum or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years, to a fine or to both.

(4) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

226IE Part 7B: interpretation

(1) In this Part—

"personal data" has the same meaning as in Part 7 (see section 199(2));

"protected data" has the same meaning as in Part 7 (see section 203);

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of His Majesty's Diplomatic Service;

"third party BPD warrant" has the meaning given by section 226F.

(3) See also—

section 263 (general definitions),

section 265 (index of defined expressions)."

Minor and consequential amendments

6 Minor and consequential amendments

(1) The Investigatory Powers Act 2016 is amended in accordance with subsections (2) to (4).

(2) In section 1 (overview of Act), in subsection (6)—

(a) in the words before paragraph (a), for "Parts 2 to 7" substitute "Parts 2 to 7B";

(b) in paragraph (e)—

(i) for "Part 7 deals" substitute "Parts 7 to 7B deal";

(ii) after "warrants" insert "and authorisations".

(3) In section 2 (general duties in relation to privacy), in subsection (1)—

(a) in paragraph (a), for "or 7" substitute ", 7 or 7B";

(b) omit the "or" after paragraph (j);

(c) after that paragraph insert—

"(ja) to grant, renew or cancel an authorisation under Part 7A,

(jb) to approve a decision to grant or renew such an authorisation, or";

(d) in paragraph (k), for "or (i)" substitute ", (i) or (ja)".

(4) In section 229 (main oversight functions), in subsection (9), in the definition of "bulk personal dataset", after "199" insert "(and includes a third party bulk personal dataset (see section 226E))".

(5) Section 65 of the Regulation of Investigatory Powers Act 2000 (the Tribunal) is amended as follows.

(6) In subsection (5)—

(a) after paragraph (czh) insert—

"(czha) the granting or renewal of an authorisation under Part 7A of that Act (low or no expectation of privacy bulk personal datasets);

(czhb) the issue, renewal or service of a warrant under Part 7B of that Act (third party bulk personal datasets);";

(b) in paragraph (czl)(i)—

(i) for "or 7" substitute ", 7 or 7B";

(ii) after "Part 3" insert "or 7A".

(7) In subsection (7ZB), after "(czh)" insert ", (czha), (czhb)".

(8) In subsection (8)—

(a) in paragraph (a), for "or 7" substitute ", 7 or 7B";

(b) after paragraph (bb) insert—

"(bba) an authorisation under Part 7A of that Act;".

PART 2

OVERSIGHT ARRANGEMENTS

7 Deputy Investigatory Powers Commissioners

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 227 (Investigatory Powers Commissioner and other Judicial Commissioners), after subsection (6) insert—

"(6A) The Investigatory Powers Commissioner may appoint up to two persons who are Judicial Commissioners to be Deputy Investigatory Powers Commissioners.

(6B) A person appointed as a Deputy Investigatory Powers Commissioner continues to be a Judicial Commissioner."

(3) In section 228 (terms and conditions of appointment), after subsection (5) insert—

"(6) A person ceases to be a Deputy Investigatory Powers Commissioner if—

(a) the person ceases to be a Judicial Commissioner,

(b) the Investigatory Powers Commissioner removes the person from being a Deputy Investigatory Powers Commissioner, or

(c) the person resigns as a Deputy Investigatory Powers Commissioner."

(4) In section 263(1) (general definitions), at the appropriate place insert—

""Deputy Investigatory Powers Commissioner" means a person appointed under section 227(6A) (and the expression is also to be read in accordance with section 227(13)(b)),".

(5) In section 265 (index of defined expressions), in the table, at the appropriate place insert—

"Deputy Investigatory Powers Commissioner	Section 263(1)".

8 Delegation of functions

(1) Section 227 of the Investigatory Powers Act 2016 (Investigatory Powers Commissioner and other Judicial Commissioners) is amended in accordance with subsections (2) to (6).

(2) For subsections (8) and (9) substitute—

"(8) The Investigatory Powers Commissioner may, to such extent as the Investigatory Powers Commissioner may decide, delegate the exercise of functions of the Investigatory Powers Commissioner to—

(a) a Deputy Investigatory Powers Commissioner, or

(b) any other Judicial Commissioner.

This is subject to subsections (8A) to (8C).

(8A) Subsection (8)(a) applies to the function of the Investigatory Powers Commissioner of—

(a) making a recommendation under subsection (4)(e),

(b) deciding under section 90(11) or 257(10) whether to approve a decision of the Secretary of State,

(c) making an appointment under section 228A(2) or 247(1), or

(d) deciding—

(i) an appeal against, or a review of, a decision made by another Judicial Commissioner, and

(ii) any action to take as a result,

only where the Investigatory Powers Commissioner is unable or unavailable to exercise the function for any reason.

(8B) Subsection (8)(b) does not apply to any function of the Investigatory Powers Commissioner mentioned in subsection (8A).

(8C) Subsection (8) does not apply to the function of the Investigatory Powers Commissioner of making an appointment under subsection (6A).

(8D) Where there are two Deputy Investigatory Powers Commissioners, the power in subsection (8)(a) may, in particular, be used to delegate to one Deputy Investigatory Powers Commissioner the exercise of the function of the Investigatory Powers Commissioner of deciding—

(a) an appeal against, or a review of, a decision made by the other Deputy Investigatory Powers Commissioner, and

(b) any action to take as a result."

(3) Omit subsection (9A) (authorisations for obtaining communications data).

(4) After subsection (10) insert—

"(10A) Where—

(a) the exercise of a function of the Investigatory Powers Commissioner mentioned in subsection (8A)(d) is delegated to a Deputy Investigatory Powers Commissioner in accordance with subsection (8)(a), and

(b) the Deputy Investigatory Powers Commissioner decides the appeal or review (and any action to take as a result),

no further appeal, or request for a further review, may be made to the Investigatory Powers Commissioner in relation to the decision of the Deputy Investigatory Powers Commissioner."

(5) In subsection (13), for paragraph (b) substitute—

"(b) to the Investigatory Powers Commissioner are to be read—

(i) so far as necessary for the purposes of subsection (8)(a), as references to the Investigatory Powers Commissioner or any Deputy Investigatory Powers Commissioner, and

(ii) so far as necessary for the purposes of subsection (8)(b), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner."

(6) After subsection (13) insert—

"(14) In this section a reference to deciding an appeal against, or a review of, a decision made by a Judicial Commissioner includes a reference to deciding whether to approve a decision that the Judicial Commissioner has refused to approve."

(7) In section 238(6)(a) of the Investigatory Powers Act 2016 (funding, staff and facilities etc), after "section", in the second place it occurs, insert "227(6A), 228A(2) or".

9 Temporary Judicial Commissioners

After section 228 of the Investigatory Powers Act 2016 (but before the italic heading before section 229) insert—

"**228A Temporary Judicial Commissioners**

(1) The power in subsection (2) is exercisable where the Investigatory Powers Commissioner and the Secretary of State consider that—

(a) as a result of exceptional circumstances, there is a shortage of persons able to carry out Judicial Commissioner functions, and

(b) the power in subsection (2) needs to be exercised in order to deal with that shortage.

(2) The Investigatory Powers Commissioner may appoint one or more persons to carry out Judicial Commissioner functions.

(3) A person appointed under subsection (2) is referred to in this section as a "temporary Judicial Commissioner".

(4) A temporary Judicial Commissioner may be appointed under subsection (2) for one or more terms not exceeding six months each and not exceeding three years in total.

(5) As soon as practicable after the appointment of any temporary Judicial Commissioner, the Investigatory Powers Commissioner must notify the following persons of the appointment—

(a) the Prime Minister;

(b) the Secretary of State;

(c) the Scottish Ministers;

(d) the Lord Chancellor;

(e) the Lord Chief Justice of England and Wales;

(f) the Lord President of the Court of Session;

(g) the Lord Chief Justice of Northern Ireland.

(6) A reference to a Judicial Commissioner in any enactment (including this Act) is to be read (so far as the context allows) as referring also to a temporary Judicial Commissioner.

(7) But subsections (1) and (4) to (6) of section 227 and section 228(2) (appointment requirements etc) do not apply in relation to temporary Judicial Commissioners.

(8) In this section "Judicial Commissioner functions" means the functions conferred on Judicial Commissioners by any enactment (including this Act)."

10 Main functions of the Investigatory Powers Commissioner

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 229 (main oversight functions)—

(a) in subsection (3), omit paragraph (c) (prevention or restriction of use of communication devices by prisoners etc);

(b) after subsection (3D) insert—

"(3E) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) compliance by any part of His Majesty's forces, or by any part of the Ministry of Defence, with policies governing—

(a) the use of surveillance outside the United Kingdom, and

(b) the use and conduct of covert human intelligence sources outside the United Kingdom,

(whether or not authorised under the Regulation of Investigatory Powers Act 2000)."

(3) In section 230 (additional directed oversight functions), in subsection (1)—

(a) omit the "or" after paragraph (b);

(b) after paragraph (c) insert ", or

(d) any public authority not mentioned in paragraphs (a) to (c), or any part of such an authority, so far as engaging in intelligence activities."

(4) In section 231 (error reporting)—

(a) in subsection (9)(b), for "code of practice under Schedule 7" substitute "relevant code of practice";

(b) after subsection (9) insert—

"(10) In subsection (9) "relevant code of practice" means a code of practice under—

(a) Schedule 7,

(b) the Police Act 1997,

(c) the Regulation of Investigatory Powers Act 2000, or

(d) the Regulation of Investigatory Powers (Scotland) Act 2000."

11 Personal data breaches

(1) In the Investigatory Powers Act 2016, after section 235 insert—

"**235A Personal data breaches**

(1) This section applies where a telecommunications operator would, but for a relevant restriction, be required by regulation 5A(2) of the 2003 Regulations to notify a personal data breach to the Information Commissioner.

(2) The telecommunications operator must report the personal data breach to the Investigatory Powers Commissioner.

(3) Where a telecommunications operator reports a personal data breach to the Investigatory Powers Commissioner under subsection (2), a Judicial Commissioner must disclose information about the breach to the Information Commissioner.

(4) Where a Judicial Commissioner discloses information about a personal data breach to the Information Commissioner under subsection (3), the Information Commissioner must—

(a) consider whether the breach is serious, and

(b) if the Information Commissioner considers that the breach is serious, notify the Investigatory Powers Commissioner.

(5) The Investigatory Powers Commissioner must inform an individual of any personal data breach relating to that individual of which the Commissioner is notified under subsection (4)(b) if the Commissioner considers that it is in the public interest for the individual to be informed of the breach.

(6) In making a decision under subsection (5), the Investigatory Powers Commissioner must, in particular, consider—

(a) the seriousness of the breach and its effect on the individual concerned, and

(b) the extent to which disclosing the breach would be contrary to the public interest or prejudicial to—

(i) national security,

(ii) the prevention or detection of serious crime,

(iii) the economic well-being of the United Kingdom, or

(iv) the continued discharge of the functions of any of the intelligence services.

(7) Before making a decision under subsection (5), the Investigatory Powers Commissioner must ask—

(a) the Secretary of State, and

(b) any public authority that the Investigatory Powers Commissioner considers appropriate,

to make submissions to the Commissioner about the matters concerned.

(8) When informing an individual under subsection (5) of a breach, the Investigatory Powers Commissioner must—

(a) inform the individual of any rights that the individual may have to apply to the Investigatory Powers Tribunal in relation to the breach, and

(b) provide such details of the breach as the Commissioner considers to be necessary for the exercise of those rights, having regard in

particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (6)(b)(i) to (iv).

(9) The Investigatory Powers Commissioner may not inform the individual to whom it relates of a personal data breach notified to the Commissioner under subsection (4)(b) except as provided by this section.

(10) For the purposes of this section, a personal data breach is serious if the breach is likely to result in a high risk to the rights and freedoms of individuals.

(11) In this section—

"2003 Regulations" means the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426);

"personal data breach" has the same meaning as in the 2003 Regulations (see regulation 2(1) of those Regulations);

"relevant restriction" means any of the following—

(a) section 57(1) (duty not to make unauthorised disclosures) (including as applied by section 156);

(b) section 132(1) (duty not to make unauthorised disclosures) (including as applied by section 197);

(c) section 174(1) (offence of making unauthorised disclosure),

(read with regulation 29(1)(a)(i) of the 2003 Regulations)."

(2) In section 65 of the Regulation of Investigatory Powers Act 2000 (the Tribunal)—

(a) in subsection (2), after paragraph (b) insert—

"(ba) to consider and determine any complaints made to them which, in accordance with subsection (4AA), are complaints for which the Tribunal is the appropriate forum;";

(b) after subsection (4) insert—

"(4AA) The Tribunal is the appropriate forum for a complaint if it is a complaint by an individual about a relevant personal data breach.

(4AB) In subsection (4AA) "relevant personal data breach" means a personal data breach that the individual is informed of under section 235A(5) of the Investigatory Powers Act 2016 (serious personal data breaches)."

(3) In section 67 of the Regulation of Investigatory Powers Act 2000 (exercise of the Tribunal's jurisdiction)—

(a) in subsection (1)(b), after "65(2)(b)" insert ", (ba)";

(b) in subsection (5)—

(i) the words from "section" to the end become paragraph (a), and

(ii) after that paragraph insert ", or

(b) section 65(2)(ba) if it is made more than one year after the personal data breach to which it relates.";

(c) in subsection (6), for "reference" substitute "complaint or reference has been".

(4) In section 68 of the Regulation of Investigatory Powers Act 2000 (Tribunal procedure), for subsection (8) substitute—

"(8) In this section "relevant Commissioner" means—

(a) the Investigatory Powers Commissioner or any other Judicial Commissioner,
(b) the Investigatory Powers Commissioner for Northern Ireland, or
(c) the Information Commissioner."

(5) In regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426) (personal data breach), omit paragraph (9) (notification to the Investigatory Powers Commissioner).

(6) In consequence of subsection (5), in Schedule 10 to the Investigatory Powers Act 2016 (minor and consequential provision), omit paragraph 14 (personal data breach) and the italic heading before it.

PART 3

COMMUNICATIONS DATA ETC

Communications data

12 Offence of unlawfully obtaining communications data

(1) Section 11 of the Investigatory Powers Act 2016 (offence of unlawfully obtaining communications data) is amended in accordance with subsections (2) and (3).

(2) In subsection (1) for the words from "from" to the end substitute "from—
(a) a telecommunications operator which is not wholly or mainly funded out of public funds, or
(b) a postal operator,

is guilty of an offence."

(3) After subsection (3) insert—

"(3A) The following are examples of cases where a relevant person has lawful authority to obtain communications data from a telecommunications operator or postal operator—
(a) where the relevant person's obtaining of the communications data is lawful for all purposes in accordance with section 81(1);
(b) any other case where the relevant person obtains the communications data in the exercise of a statutory power of the relevant public authority;
(c) where the operator lawfully provides the communications data to the relevant person otherwise than pursuant to the exercise of a statutory power of the relevant public authority (whether or not in the exercise of a statutory power to disclose);
(d) where the communications data is obtained in accordance with a court order or other judicial authorisation;
(e) where the communications data had been published before the relevant person obtained it;

(f) where the communications data is obtained by the relevant person for the purpose of enabling, or facilitating, the making of a response to a call made to the emergency services.

(3B) In subsection (3A)—

"emergency services" means—

(a) police, fire, rescue and ambulance services, and

(b) His Majesty's Coastguard;

"publish" means make available to the public or a section of the public (whether or not on a commercial basis)."

(4) In section 6 of that Act, in the heading, at the end insert "in relation to interceptions".

(5) The amendments made by subsections (1) to (3) have effect only in relation to the obtaining of communications data after this section comes into force.

13 Meaning of "communications data": subscriber details

(1) Section 261 of the Investigatory Powers Act 2016 (telecommunications definitions) is amended as follows.

(2) In subsection (5), in the words after paragraph (c), after "but" insert "(subject to subsection (5A))".

(3) After subsection (5) insert—

"(5A) In subsection (5) the words after paragraph (c) do not apply to relevant subscriber data.

(5B) In subsection (5A) "relevant subscriber data" means entity data, other than data comprised in a recording of speech, which—

(a) constitutes any or all of the content of a communication made for the purpose of initiating or maintaining an entity's access to a telecommunications service, and

(b) is about an entity to which that telecommunications service is (or is to be) provided."

14 Powers to obtain communications data

(1) Section 12 of the Investigatory Powers Act 2016 (abolition or restriction of certain powers to obtain communications data) is amended in accordance with subsections (2) to (6).

(2) In subsection (2)(b) omit "and is not a regulatory power or a relevant postal power".

(3) In subsection (2A), at the end insert "and subsection (2B)".

(4) After subsection (2A) insert—

"(2B) Subsection (2) does not apply to the exercise by a specified public authority, otherwise than in the course of a criminal investigation, of a general information power which is a regulatory or supervisory power.

(2C) For the purposes of subsection (2B), "criminal investigation" means an investigation of any criminal conduct, including—

(a) an investigation of alleged or suspected criminal conduct, and

(b) an investigation of whether criminal conduct has taken place.

(2D) For the purposes of subsection (2B), the exercise of a general information power which is a regulatory or supervisory power is treated as not being in the course of a criminal investigation if at the time of the exercise of the power the investigation is not being conducted with a view to seeking a criminal prosecution."

(5) Omit subsection (3).

(6) After subsection (5) insert—

"(5A) In this section "specified public authority" means a public authority which is—

(a) listed in Schedule 2A, or

(b) listed in column 1 of the table in Schedule 4.

(5B) The Secretary of State or the Treasury may by regulations modify Schedule 2A by—

(a) adding a public authority to, or

(b) removing a public authority from,

the list in that Schedule."

(7) In subsection (6)—

(a) at the appropriate place insert—

""criminal conduct" means conduct which constitutes an offence under the law of any part of the United Kingdom,";

(b) for the definition of "regulatory power" substitute—

""regulatory or supervisory power" means any power (however expressed) to obtain information or documents which—

(a) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(b) is exercisable in connection with—

(i) the regulation of persons or activities,

(ii) the checking or monitoring of compliance with requirements, prohibitions or standards imposed by or under an enactment, or

(iii) the enforcement of any requirement or prohibition imposed by or under an enactment,";

(c) omit the definition of "relevant postal power".

(8) In section 267 of the Investigatory Powers Act 2016 (regulations), in subsection (5), after paragraph (a) insert—

"(aa) regulations under section 12(5B),".

(9) In the Investigatory Powers Act 2016, after Schedule 2 insert—

"SCHEDULE 2A Section 12(5A)

SPECIFIED PUBLIC AUTHORITIES FOR THE PURPOSES OF SECTION 12

1 The Treasury.

2 A local authority.

In this Schedule "local authority" has the same meaning as in Part 3 (see section 86)."

(10) The Schedule reverses the effect of certain repeals of disclosure powers, and makes consequential and supplementary provision.

Internet connection records

15 Internet connection records

(1) Section 62 of the Investigatory Powers Act 2016 (restrictions in relation to internet connection records) is amended as follows.

(2) In subsection (A2) for "or C" substitute ", C or D1".

(3) In subsection (2)—

(a) after "authorisation" insert "under section 61 or 61A";

(b) for "or C" substitute ", C or D2".

(4) After subsection (5) insert—

"(5A) Condition D1 is that—

(a) the application is made by a relevant public authority which is specified in column 1 of the table (see below), and

(b) the Investigatory Powers Commissioner considers that it is necessary, for a purpose described in the corresponding entry in column 2 of the table, to identify which persons or apparatuses are using one or more specified internet services in a specified period.

1 (applicant)	*2 (description(s) of purpose)*
Security Service, Secret Intelligence Service or GCHQ	A purpose falling within subsection (7)(a) or (c) of section 60A, or falling within subsection (7)(b) of that section by virtue of subsection (8)(a) of that section.
National Crime Agency	A purpose falling within subsection (7)(b) of section 60A by virtue of subsection (8)(a) of that section.

(5B) Condition D2 is that—

(a) the relevant public authority whose designated senior officer has power to grant the authorisation is specified in column 1 of the table (see below), and

(b) that officer considers that it is necessary, for a purpose described in the corresponding entry in column 2 or 3 of the table (as applicable), to identify which persons or apparatuses are using one or more specified internet services in a specified period.

1 (relevant public authority)	*2 (description of purpose: authorisation under section 61)*	*3 (description of purpose: authorisation under section 61A)*
Security Service, Secret Intelligence Service or GCHQ	A purpose falling within section 61(7)(a) or (c).	A purpose falling within subsection (7)(a) of section 61A by virtue of subsection (8)(a) of that section.
National Crime Agency		A purpose falling within subsection (7)(a) of section 61A by virtue of subsection (8)(a) of that section.

(5C) In subsections (5A)(b) and (5B)(b) "specified" means specified in the application for the authorisation."

PART 4

NOTICES

Retention notices

16 Powers to require retention of certain data

(1) Section 87 of the Investigatory Powers Act 2016 (powers to require retention of certain data) is amended as follows.

(2) In subsection (4)—

(a) in the words before paragraph (a), after "data" insert ", other than data which is, or can only be obtained by processing, an internet connection record,";

(b) in paragraph (a), after "provided" insert "(solely or jointly with another person)";

(c) after paragraph (a) insert—

"(aa) does not relate to a relevant roaming service,".

(3) After subsection (4) insert—

"(4A) In subsection (4) "relevant roaming service" means a telecommunications service provided by the system operator under an agreement with a telecommunications operator outside the United Kingdom (the "non-UK operator") which facilitates the use by persons in the United Kingdom of the system operator's telecommunication system to access one or more telecommunications services of the non-UK operator."

(4) In subsection (11), in the words after paragraph (e)—

(a) for "and" substitute "(and";

(b) for "records" substitute "records)".

17 Extra-territorial enforcement of retention notices etc

(1) Part 4 of the Investigatory Powers Act 2016 is amended as follows.

(2) In section 95 (enforcement of notices and certain other requirements and restrictions), in subsection (5), after "enforceable" insert "(whether or not the person is in the United Kingdom)".

(3) In section 97 (extra-territorial application of Part 4), omit subsection (2).

Retention, national security and technical capability notices

18 Review of notices by the Secretary of State

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 90 (retention notices: review by the Secretary of State)—

(a) for subsection (4) substitute—

"(4) Where a telecommunications operator refers a retention notice under subsection (1)—

(a) there is no requirement for the operator to comply with the notice, so far as referred, and

(b) subsection (4A) applies to the operator,

until the Secretary of State has reviewed the notice in accordance with subsection (5).

(4A) Where this subsection applies to a telecommunications operator, the operator must not make any relevant changes to telecommunications services or telecommunication systems to which obligations imposed by the retention notice relate.

(4B) In subsection (4A) "relevant change" means a change that, if implemented, would have a negative effect on the capability of the operator to provide any assistance which the operator may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act.";

(b) in subsection (5)—

(i) after "must" insert ", before the end of the review period,";

(ii) after "(1)" insert "(and accordingly decide what action to take under subsection (10))";

(c) after subsection (5) insert—

"(5A) In subsection (5) "the review period" means—

(a) such period as may be provided for by regulations made by the Secretary of State, or

(b) if that period is extended by the Secretary of State in accordance with the regulations (see subsection (14)), such extended period.";

(d) after subsection (9) insert—

"(9A) The Commissioner may give a direction to the operator concerned or the Secretary of State specifying the period within which the operator

or the Secretary of State (as the case may be) may provide evidence, or make representations, in accordance with subsection (9)(a).

(9B) If the Commissioner gives such a direction to the operator or the Secretary of State, the Board and the Commissioner are not required to take into account any evidence provided, or representations made, by the operator or the Secretary of State (as the case may be) after the end of that period.";

(e) in subsection (10)—

(i) for "may" substitute "must";

(ii) after "Commissioner" insert "but before the end of the relevant period, decide whether to";

(f) after subsection (11) insert—

"(11A) In subsection (10) "the relevant period" means—

(a) such period as may be provided for by regulations made by the Secretary of State, or

(b) if that period is extended by the Secretary of State in accordance with the regulations (see subsection (15)), such extended period.";

(g) after subsection (13) insert—

"(14) Regulations under subsection (5A)(a) may include provision enabling any period provided for by the regulations to be extended by the Secretary of State where the extension is agreed by the Secretary of State, the telecommunications operator concerned and a Judicial Commissioner.

(15) Regulations under subsection (11A)(a) may include provision enabling any period provided for by the regulations to be extended by the Secretary of State—

(a) where the Secretary of State considers that there are exceptional circumstances that justify the extension, or

(b) in any other circumstances specified in the regulations.

(16) Where regulations under subsection (11A)(a) include provision mentioned in subsection (15), the regulations must also include provision requiring the Secretary of State to notify a Judicial Commissioner and the telecommunications operator concerned of the duration of any extended period."

(3) In section 95(5) (enforcement of retention notices etc), after "or (2)" insert ", or under section 90(4A),".

(4) In section 255(10) (enforcement of national security notices and technical capability notices), in the opening words, for "subsection (9)" substitute "subsection (8) or (9), or by section 257(3A),".

(5) In section 257 (national security notices and technical capability notices: review by the Secretary of State)—

(a) for subsection (3) substitute—

"(3) Where a person who is given a notice under section 252 or 253 refers the notice under subsection (1)—

(a) there is no requirement for the person to comply with the notice, so far as referred, and

(b) subsection (3A) applies to the person,

until the Secretary of State has reviewed the notice in accordance with subsection (4).

(3A) Where this subsection applies to a person, the person must not make any relevant changes to telecommunications or postal services, or telecommunication systems, to which obligations imposed by the notice given under section 252 or 253 relate.

(3B) In subsection (3A) "relevant change" means a change that, if implemented, would have a negative effect on the capability of the person to provide any assistance which the person may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act.";

(b) in subsection (4)—

(i) after "must" insert ", before the end of the review period,";

(ii) after "(1)" insert "(and accordingly decide what action to take under subsection (9))";

(c) after subsection (4) insert—

"(4A) In subsection (4) "the review period" means—

(a) such period as may be provided for by regulations made by the Secretary of State, or

(b) if that period is extended by the Secretary of State in accordance with the regulations (see subsection (13)), such extended period.";

(d) after subsection (8) insert—

"(8A) The Commissioner may give a direction to the person concerned or the Secretary of State specifying the period within which the person or the Secretary of State (as the case may be) may provide evidence, or make representations, in accordance with subsection (8)(a).

(8B) If the Commissioner gives such a direction to the person or the Secretary of State, the Board and the Commissioner are not required to take into account any evidence provided, or representations made, by the person or the Secretary of State (as the case may be) after the end of that period.";

(e) in subsection (9)—

(i) for "may" substitute "must";

(ii) after "Commissioner" insert "but before the end of the relevant period, decide whether to";

(f) after subsection (10) insert—

"(10A) In subsection (9) "the relevant period" means—

(a) such period as may be provided for by regulations made by the Secretary of State, or

(b) if that period is extended by the Secretary of State in accordance with the regulations (see subsection (14)), such extended period.";

(g) after subsection (12) insert—

"(13) Regulations under subsection (4A)(a) may include provision enabling any period provided for by the regulations to be extended by the Secretary of State where the extension is agreed by the Secretary of State, the person concerned and a Judicial Commissioner.

(14) Regulations under subsection (10A)(a) may include provision enabling any period provided for by the regulations to be extended by the Secretary of State—

(a) where the Secretary of State considers that there are exceptional circumstances that justify the extension, or

(b) in any other circumstances specified in the regulations.

(15) Where regulations under subsection (10A)(a) include provision mentioned in subsection (14), the regulations must also include provision requiring the Secretary of State to notify a Judicial Commissioner and the person concerned of the duration of any extended period."

(6) In section 267(3) (regulations: affirmative procedure)—

(a) in paragraph (e), after "90(1)" insert ", (5A)(a) or (11A)(a)";

(b) in paragraph (j), after "257(1)" insert ", (4A)(a) or (10A)(a)".

19 Meaning of "telecommunications operator" etc

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 261(10) (meaning of "telecommunications operator")—

(a) omit the "or" after paragraph (a);

(b) after paragraph (b) insert ", or

(c) controls or provides a telecommunication system which—

(i) is not (wholly or partly) in, or controlled from, the United Kingdom, and

(ii) is used by another person to offer or provide a telecommunications service to persons in the United Kingdom."

(3) In section 253 (technical capability notices)—

(a) in subsection (1)(a)—

(i) after "the operator", in the first place it occurs, insert "or another relevant operator";

(ii) for "the operator", in the second place it occurs, substitute "such operator";

(b) in subsection (2)(a), after "operator" insert "(to whom the notice is given)".

20 Renewal of notices

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) In section 87 (powers to require retention of certain data), after subsection (6) insert—

"(6A) A retention notice ceases to have effect at the end of the relevant period unless before the end of that period—

(a) it is varied in accordance with section 94(4) so as to require the retention of additional relevant communications data,

(b) it is renewed (see section 94A), or

(c) it is revoked or otherwise ceases to have effect (see sections 90(10) and 94).

(6B) In subsection (6A) the "relevant period" means the period of two years beginning with—

(a) in the case of a retention notice that has not been varied as mentioned in subsection (6A)(a) or renewed, the day on which the notice comes into force, or

(b) in the case of a retention notice that has been so varied or renewed, the day after the day at the end of which the retention notice would have ceased to have effect if it had not been so varied or renewed."

(3) In the italic heading before section 94, for "or revocation" substitute ", revocation or renewal".

(4) After section 94 (but before the italic heading before section 95) insert—

"**94A Renewal of notices**

(1) If the renewal conditions are met, a retention notice may be renewed, at any time during the renewal period, by a notice given by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the requirement in the retention notice for a telecommunications operator to retain relevant communications data is still necessary and proportionate for one or more of the purposes falling within sub-paragraphs (i) to (vi) of section 87(1)(a), and

(b) that the decision to renew the notice has been approved by a Judicial Commissioner.

(3) The renewal period means the period of 30 days ending with the day at the end of which the retention notice would otherwise cease to have effect.

(4) The Secretary of State must give, or publish, notice of the renewal in such manner as the Secretary of State considers appropriate for bringing the renewal to the attention of the telecommunications operator (or description of operators) to whom it relates.

(5) Sections 87(10), 88, 89 and 90 apply in relation to the renewal of a retention notice as they apply in relation to the giving of a retention notice."

(5) In section 229 (main oversight functions), in subsection (8)(e)(i), for "or varying" substitute ", varying or renewal".

(6) In section 255 (further provision about national security notices and technical capability notices), after subsection (5) insert—

"(5A) A relevant notice ceases to have effect at the end of the relevant period unless before the end of that period—

(a) it is varied in accordance with section 256(4)(c) or (5)(c) so as to impose further requirements on the person to whom the notice was given,

(b) it is renewed (see section 256A), or

(c) it is revoked or otherwise ceases to have effect (see section 256).

(5B) In subsection (5A) the "relevant period" means the period of two years beginning with—

(a) in the case of a relevant notice that has not been varied as mentioned in subsection (5A)(a) or renewed, the day on which the notice was given, or

(b) in the case of a relevant notice that has been so varied or renewed, the day after the day at the end of which the relevant notice would have ceased to have effect if it had not been so varied or renewed."

(7) After section 256 insert—

"**256A Renewal of notices**

(1) If the renewal conditions are met, a relevant notice may be renewed, at any time during the renewal period, by a notice given by the Secretary of State.

(2) The renewal conditions for a national security notice given under section 252 are that—

(a) the Secretary of State considers that the notice is still necessary in the interests of national security,

(b) the Secretary of State considers that the conduct required by the notice is still proportionate to what is sought to be achieved by that conduct, and

(c) the decision to renew the notice has been approved by a Judicial Commissioner.

(3) The renewal conditions for a technical capability notice given under section 253 are that—

(a) the Secretary of State considers that the notice is still necessary for securing that the relevant operator has the capability to provide any assistance which the operator may be required to provide in relation to any relevant authorisation,

(b) the Secretary of State considers that the conduct required by the notice is still proportionate to what is sought to be achieved by that conduct, and

(c) the decision to renew the notice has been approved by a Judicial Commissioner.

(4) The renewal period means the period of 30 days ending with the day at the end of which the relevant notice would otherwise cease to have effect.

(5) If the Secretary of State renews a relevant notice given to any person, the Secretary of State must give that person notice in writing of the renewal.

(6) Sections 254, 255(2) to (4) and (7) and 257 apply in relation to the renewal of a relevant notice as they apply in relation to the giving of a relevant notice.

(7) Section 255(6) applies to any notice of the renewal of a technical capability notice as it applies to a technical capability notice.

(8) In this section—

"relevant authorisation" has the meaning given by section 253;

"relevant notice" means—

(a) a national security notice under section 252, or

(b) a technical capability notice under section 253;

"relevant operator" has the meaning given by section 253."

Notification of proposed changes to telecommunications services etc

21 Notification of proposed changes to telecommunications services etc

(1) The Investigatory Powers Act 2016 is amended in accordance with subsections (2) and (3).

(2) After section 258 (but before the italic heading before section 259) insert—

"**258A Notification of proposed changes to telecommunications services etc**

(1) The Secretary of State may give a relevant operator a notice in writing under this section requiring the operator to notify the Secretary of State of any proposals of the operator to make any relevant changes specified in the notice.

(2) In this section "relevant change" means a change—

(a) to a service or system within subsection (3), and

(b) that is specified in regulations made by the Secretary of State as a change that may be included in a notice given under this section.

(3) The following are within this subsection—

(a) telecommunications services offered or provided by the operator;

(b) telecommunication systems controlled or provided by the operator;

(c) postal services provided by the operator.

(4) Regulations under subsection (2) may in particular specify changes by reference to the impact of the changes on the capability of a relevant operator to provide any assistance which the operator may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act.

(5) The Secretary of State may give a relevant operator a notice under this section only if the Secretary of State considers that—

(a) the notice is necessary for maintaining the capability of the relevant operator to provide any assistance which the operator may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act, and

(b) the conduct required by the notice is proportionate to what is sought to be achieved by that conduct.

(6) Before giving a notice under this section, the Secretary of State must among other matters take into account—

(a) the likely benefits of the notice,

(b) the likely number of users (if known) of any postal or telecommunications service to which the notice relates,

(c) the likely cost of complying with the notice, and

(d) any other effect of the notice on the operator to whom it relates.

(7) Before giving a notice under this section to a relevant operator, the Secretary of State must consult that operator.

(8) A relevant operator to whom a notice is given under this section, or any person employed or engaged for the purposes of that relevant operator's business, must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State.

(9) A relevant operator to whom a notice is given under this section must comply with the notice a reasonable time before making any relevant changes to which the notice relates.

(10) The duty imposed by subsection (8) or (9) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(11) In this section "relevant operator" means—

(a) a postal operator,

(b) a telecommunications operator, or

(c) a person who is proposing to become a postal operator or a telecommunications operator,

who meets the condition in subsection (12).

(12) The condition in this subsection is that the operator or person provides (or has provided) assistance in relation to any warrant, authorisation or notice issued or given under this Act.

258B Variation and revocation of notices given under section 258A

(1) In this section—

"relevant notice" means a notice given under section 258A;

"relevant operator" has the same meaning as in that section.

(2) The Secretary of State may—

(a) vary a relevant notice;

(b) revoke a relevant notice (whether wholly or in part).

(3) The Secretary of State may vary a relevant notice only if the Secretary of State considers that—

(a) the variation is necessary for maintaining the capability of the relevant operator to provide any assistance which the operator may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act, and

(b) the conduct required by the notice, as varied, is proportionate to what is sought to be achieved by that conduct.

(4) If the Secretary of State varies or revokes a relevant notice given to any relevant operator, the Secretary of State must give that relevant operator notice in writing of the variation or revocation.

(5) The fact that a relevant notice has been revoked in relation to a particular relevant operator does not prevent the giving of another relevant notice of the same kind in relation to the same relevant operator.

(6) Subsections (6) and (7) of section 258A apply in relation to varying or revoking a relevant notice as they apply in relation to giving a relevant notice.

(7) Any reference in this section or section 258A(8) or (9) to a notice given under section 258A includes a reference to such a notice as varied under this section."

(3) In section 267(3) (regulations)—

(a) omit the "or" after paragraph (j);

(b) after that paragraph insert—

"(ja) section 258A(2), or".

(4) The Regulation of Investigatory Powers Act 2000 is amended as follows.

(5) In section 65 (the Tribunal)—

(a) in subsection (5)(czi)—

(i) for "or 253" substitute ", 253 or 258A";

(ii) for "or technical capability" substitute ", technical capability or proposed changes to telecommunications services etc";

(b) in subsection (5)(czl)(iii), for "or 253" substitute ", 253 or 258A";

(c) in subsection (8)(bc), for "or 253" substitute ", 253 or 258A".

(6) In section 67 (exercise of the Tribunal's jurisdiction), in subsection (7)(azc), for "or 253" substitute ", 253 or 258A".

(7) In section 68 (Tribunal procedure)—

(a) in subsection (5)(b), for "or 253" substitute ", 253 or 258A";

(b) in subsection (7)(f), for "or 253" substitute ", 253 or 258A";

(c) in subsection (7)(ha), for "or 253" substitute ", 253 or 258A".

PART 5

MISCELLANEOUS

Members of Parliament etc

22 Interception and examination of communications: Members of Parliament etc

(1) Section 26 of the Investigatory Powers Act 2016 (interception and examination of communications: Members of Parliament etc) is amended as follows.

(2) In subsection (2)—

(a) the words "the Prime Minister" become paragraph (a);

(b) after that paragraph insert ", or

(b) if conditions A and B are met, an individual (other than that Secretary of State) designated by the Prime Minister under this section."

(3) After subsection (2) insert—

"(2A) Condition A is that the Prime Minister is unable to decide whether to give approval under subsection (2), due to incapacity or inability to access secure communications.

(2B) Condition B is that the Secretary of State or a senior official considers that there is an urgent need for the decision (as to whether to give such approval) to be made.

(2C) The Prime Minister may designate up to five individuals under this section.

(2D) The Prime Minister may designate an individual under this section only if the individual—

(a) holds the office of Secretary of State, and

(b) has the necessary operational awareness to decide whether to give approvals under subsection (2).

(2E) A designation under this section ends—

(a) when the individual ceases to hold the office of Secretary of State, or

(b) if earlier, when revoked by the Prime Minister.

(2F) In this section "senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of His Majesty's Diplomatic Service."

23 Equipment interference: Members of Parliament etc

(1) Section 111 of the Investigatory Powers Act 2016 (equipment interference: Members of Parliament etc) is amended as follows.

(2) In subsection (3)—

(a) the words "the Prime Minister" become paragraph (a);

(b) after that paragraph insert ", or

(b) if conditions A and B are met, an individual (other than that Secretary of State) designated by the Prime Minister under this section."

(3) In subsection (6)—

(a) the words "the Prime Minister" become paragraph (a);

(b) after that paragraph insert ", or

(b) if conditions A and B are met, an individual (other than that Secretary of State) designated by the Prime Minister under this section."

(4) After subsection (7) insert—

"(7A) Condition A is that the Prime Minister is unable to decide whether to give approval under subsection (3) or (as the case may be) (6), due to incapacity or inability to access secure communications.

(7B) Condition B is that the Secretary of State or a senior official considers that there is an urgent need for the decision (as to whether to give such approval) to be made.

(7C) The Prime Minister may designate up to five individuals under this section.

(7D) The Prime Minister may designate an individual under this section only if the individual—

(a) holds the office of Secretary of State, and

(b) has the necessary operational awareness to decide whether to give approvals under subsection (3) or (6).

(7E) A designation under this section ends—

(a) when the individual ceases to hold the office of Secretary of State, or

(b) if earlier, when revoked by the Prime Minister."

Equipment interference

24 Issue of equipment interference warrants

(1) Part 1 of the table in Schedule 6 to the Investigatory Powers Act 2016 (issue of warrants under section 106 etc) is amended in accordance with subsections (2) and (3).

(2) In the entry relating to the Chief Constable of a police force maintained under section 2 of the Police Act 1996, in the second column—

(a) for "section 12A(1) of the Police Act 1996" substitute "section 41(1) of the Police Reform and Social Responsibility Act 2011";

(b) for "section 12A(2)" substitute "section 41(5)".

(3) In the entry relating to the Director General of the National Crime Agency—

(a) in the first column, after "General" insert "or a Deputy Director General";

(b) in the second column, after "General" insert "or a Deputy Director General".

(4) In section 107(3) of the Investigatory Powers Act 2016 (restriction on issue of warrants to certain law enforcement officers)—

(a) after "General", in the first place it occurs, insert "or a Deputy Director General";

(b) after "General", in the second place it occurs, insert "or the Deputy Director General (as the case may be)".

25 Modification of equipment interference warrants

In section 121 of the Investigatory Powers Act 2016 (notification of modifications), after subsection (3) insert—

"(4) But subsection (3) does not apply where the modification—

(a) is made in accordance with section 119(1), and

(b) is to remove any matter, name or description included in the warrant in accordance with section 115(3) to (5).”

26 Issue of targeted examination warrants to intelligence services

In section 102 of the Investigatory Powers Act 2016 (power to issue warrants to intelligence services: the Secretary of State), for subsection (4) substitute—

“(4) But the Secretary of State may not issue a targeted examination warrant under subsection (3) if—

(a) the Secretary of State considers that the only ground for considering the warrant to be necessary is for the purpose of preventing or detecting serious crime, and

(b) the warrant, if issued, would relate only to a person who would be in Scotland at the time of the issue of the warrant or whom the Secretary of State believes would be in Scotland at that time.

For the power of the Scottish Ministers to issue a targeted examination warrant, see section 103.”

27 Bulk equipment interference: safeguards for confidential journalistic material etc

(1) The Investigatory Powers Act 2016 is amended as follows.

(2) For section 195 (additional safeguard for confidential journalistic material) substitute—

“**195 Additional safeguards for confidential journalistic material etc**

(1) Subsection (2) applies if, in a case where material obtained under a bulk equipment interference warrant (“BEI material”) is to be selected for examination—

(a) the purpose, or one of the purposes, of using those criteria to be used for the selection of the BEI material for examination (“the relevant criteria”) is to identify any confidential journalistic material or to identify or confirm a source of journalistic information, or

(b) the use of the relevant criteria is highly likely to identify confidential journalistic material or identify or confirm a source of journalistic information.

(2) The BEI material may be selected for examination using the relevant criteria only if the use of those criteria has been approved by—

(a) the Investigatory Powers Commissioner, or

(b) in a case where a senior official acting on behalf of the Secretary of State considers there is an urgent need to do so, the senior official.

(3) The Investigatory Powers Commissioner or a senior official may give an approval under subsection (2) only if the Commissioner or official considers that—

(a) the public interest in obtaining the information that would be obtained by the selection of the BEI material for examination outweighs

the public interest in the confidentiality of confidential journalistic material or sources of journalistic information, and

(b) there are no less intrusive means by which the information may reasonably be obtained.

(4) Subsection (5) applies where—

(a) material obtained under a bulk equipment interference warrant ("the relevant material") is retained, following its examination, for purposes other than the destruction of the relevant material, and

(b) the person to whom the warrant is addressed considers that the relevant material contains confidential journalistic material or material that would identify or confirm a source of journalistic information.

(5) The person to whom the warrant is addressed must inform the Investigatory Powers Commissioner of the retention of the relevant material as soon as reasonably practicable.

(6) Unless the Investigatory Powers Commissioner considers that subsection (8) applies to the relevant material, the Commissioner must direct that the relevant material is destroyed.

(7) If the Investigatory Powers Commissioner considers that subsection (8) applies to the relevant material, the Commissioner may impose such conditions as to the use or retention of the relevant material as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of confidential journalistic material or sources of journalistic information.

(8) This subsection applies to material containing—

(a) confidential journalistic material, or

(b) material identifying or confirming a source of journalistic information,

if the public interest in retaining the material outweighs the public interest in the confidentiality of confidential journalistic material or sources of journalistic information.

(9) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsections (6) and (7), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(10) "Affected party" has the meaning given by section 194(14).

(For provision about the grounds for retaining material obtained under a warrant, see section 191.)

195A Section 195: procedure where use of criteria approved by senior official

(1) This section applies where material obtained under a bulk equipment interference warrant is selected for examination using criteria the use of which was approved by a senior official under section 195(2).

(2) The Secretary of State must, as soon as reasonably practicable, inform the Investigatory Powers Commissioner that the approval has been given.

(3) The Investigatory Powers Commissioner must, as soon as reasonably practicable—

(a) consider whether the relevant condition is met as regards the use of the criteria for the selection of the material for examination, and

(b) notify the Secretary of State of their decision.

(4) For this purpose, "the relevant condition" is that—

(a) the public interest in obtaining the information that would be obtained by the selection of the material for examination outweighs the public interest in the confidentiality of confidential journalistic material or sources of journalistic information, and

(b) there are no less intrusive means by which the information may reasonably be obtained.

(5) On the giving of a notification of a decision that the relevant condition is not met, the senior official's approval ceases to have effect.

(6) Nothing in subsection (5) affects the lawfulness of—

(a) anything done by virtue of the approval before it ceases to have effect, or

(b) if anything is in the process of being done by virtue of the approval when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop."

(3) In section 229 (main oversight functions), in subsection (8), before paragraph (g) insert—

"(fb) deciding whether—

(i) to approve the use of criteria under section 195(2)(a),

(ii) subsection 195(8) applies for the purposes of subsection 195(6) and (7),

(iii) the relevant condition is met for the purposes of subsection 195A(3)(a)."

Exclusion of matters from legal proceedings etc: exceptions

28 Exclusion of matters from legal proceedings etc: exceptions

(1) Schedule 3 to the Investigatory Powers Act 2016 (exceptions to section 56) is amended as follows.

(2) After paragraph 12 insert—

"Proceedings relating to release of prisoners etc in England and Wales

12A (1) Section 56(1) does not apply in relation to—

(a) any proceedings before the Parole Board, or

(b) any proceedings arising out of such proceedings.

(2) But sub-paragraph (1) does not permit the disclosure of anything to—

(a) any person, other than the Secretary of State, who is or was a party to the proceedings, or

(b) any person who—

(i) represents such a person for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment as a special advocate."

(3) After paragraph 24 insert—

"25 (1) Nothing in section 56(1) prohibits—

(a) a disclosure to a relevant coroner conducting an NI investigation or inquest, or

(b) a disclosure to a qualified person—

(i) appointed as legal adviser to an inquest conducted by the coroner, or

(ii) employed under section 11(3) of the Coroners Act (Northern Ireland) 1959 (c. 15) ("the 1959 Act") by a relevant coroner to assist the coroner in an investigation conducted by the coroner,

where, in the course of the investigation or inquest, the relevant coroner ("C") has ordered the disclosure to be made to C alone or (as the case may be) to C and any qualified person appointed or employed by C as mentioned in paragraph (b).

(2) A relevant coroner may order a disclosure under sub-paragraph (1) only if the coroner considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(3) In a case where a coroner ("C") conducting, or who has been conducting, an NI investigation or inquest is not a relevant coroner, nothing in section 56(1) prohibits—

(a) a disclosure to C that there is intercepted material in existence which is, or may be, relevant to the investigation or inquest;

(b) a disclosure to a qualified person appointed by C as legal adviser to the inquest or employed by C under section 11(3) of the 1959 Act to assist C in the investigation, which is made for the purposes of determining—

(i) whether any intercepted material is, or may be, relevant to the investigation, and

(ii) if so, whether it is necessary for the material to be disclosed to the person conducting the investigation.

(4) In sub-paragraph (3) "intercepted material" means—

(a) any content of an intercepted communication (within the meaning of section 56), or

(b) any secondary data obtained from a communication.

(5) In this paragraph—

"the 1959 Act" has the meaning given by sub-paragraph (1);

"coroner" means a coroner appointed under section 2 of the 1959 Act;

"NI investigation or inquest" means an investigation under section 11(1) of the 1959 Act or an inquest under section 13 or 14 of that Act;

"qualified person" means a member of the Bar of Northern Ireland, or a solicitor of the Court of Judicature of Northern Ireland);

"relevant coroner" means a coroner who is a judge of the High Court or of a county court in Northern Ireland.

26 (1) Nothing in section 56(1) prohibits—

(a) a disclosure to a relevant person conducting an inquiry under the Inquiries into Fatal Accidents and Sudden Deaths etc. (Scotland) Act 2016 (2016 asp 2) ("IFASDA 2016"), or

(b) a disclosure to a qualified person appointed under section 24 of that Act to assist a relevant person in the inquiry,

where, in the course of the inquiry, the person conducting the inquiry has ordered the disclosure to be made to that person alone or (as the case may be) to that person and any qualified person appointed to assist a relevant person in the inquiry.

(2) A relevant person may order a disclosure under sub-paragraph (1) only if the person considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(3) Nothing in section 56(1) prohibits—

(a) a disclosure to a relevant person conducting an inquiry under IFASDA 2016, or

(b) a disclosure to a qualified person appointed under section 24 of that Act to assist a relevant person in the inquiry,

that there is intercepted material in existence which is, or may be, relevant to the inquiry.

(4) In sub-paragraph (3) "intercepted material" means—

(a) any content of an intercepted communication (within the meaning of section 56), or

(b) any secondary data obtained from a communication.

(5) In this paragraph "relevant person" means—

(a) a sheriff principal,

(b) a temporary sheriff principal, or

(c) a sheriff or part-time sheriff (but not a summary sheriff or part-time summary sheriff) designated as a specialist under section 37(1) or (3) of IFASDA 2016.

(6) In this paragraph "qualified person" means an advocate or solicitor; and "advocate" and "solicitor" have the same meaning as in IFASDA 2016 (see section 40 of that Act)."

Freedom of information

29 Freedom of information: bodies dealing with security matters

In section 23(3) of the Freedom of Information Act 2000 (information supplied by, or relating to, bodies dealing with security matters), after paragraph (o) insert—

"(p) a Judicial Commissioner within the meaning of the Investigatory Powers Act 2016 (see section 263(1) of that Act)."

PART 6

GENERAL

30 Power to make consequential provision

(1) The Secretary of State may by regulations made by statutory instrument make provision that is consequential on this Act.

(2) Regulations under subsection (1) may, in particular, amend or repeal provision made by or under an Act passed before, or in the same session as, this Act.

(3) A statutory instrument containing (whether alone or with other provision) regulations under this section which amend or repeal an Act may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

(4) Any other statutory instrument containing regulations under this section is subject to annulment in pursuance of a resolution of either House of Parliament.

31 Extent

(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject as follows.

(2) Any amendment or repeal made by this Act has the same extent within the United Kingdom as the provision amended or repealed.

(3) The power under section 272(6) of the Investigatory Powers Act 2016 may be exercised so as to extend to the Isle of Man or any of the British overseas territories any amendment or repeal made by or under this Act of any part of that Act (with or without modifications).

32 Commencement.

(1) This Part comes into force on the day on which this Act is passed.

(2) The other provisions of this Act come into force on such day as the Secretary of State may by regulations made by statutory instrument appoint.

(3) Different days may be appointed for different purposes.

(4) The Secretary of State may by regulations made by statutory instrument make transitional or saving provision in connection with the coming into force of any provision of this Act.

(5) The power to make regulations under subsection (4) includes power to make different provision for different purposes.

33 Short title

This Act may be cited as the Investigatory Powers (Amendment) Act 2024.

SCHEDULE

Section 14

DISCLOSURE POWERS

PART 1

RESTORATION OF DISCLOSURE POWERS

Health and Safety at Work etc Act 1974

1 In section 20 of the Health and Safety at Work etc Act 1974 (powers of inspectors), omit subsections (9) and (10).

Criminal Justice Act 1987

2 In section 2 of the Criminal Justice Act 1987 (investigation of powers of the Director of Serious Fraud Office), omit subsections (10A) and (10B).

Consumer Protection Act 1987

3 In section 29 of the Consumer Protection Act 1987 (powers of search etc), omit subsections (8) and (9).

Environmental Protection Act 1990

4 In section 71 of the Environmental Protection Act 1990 (obtaining of information from persons and authorities), omit subsections (5) and (6).

Financial Services and Markets Act 2000

5 In section 175 of the Financial Services and Markets Act 2000 (information gathering and investigations: supplemental provision), omit subsections (5A) and (5B).

PART 2

CONSEQUENTIAL AMENDMENTS

6 In consequence of paragraphs 1 to 5 omit paragraphs 1 to 4 and 9 of Schedule 2 to the Investigatory Powers Act 2016 (abolition of disclosure powers).