Clause 1

To note: amendments that are made by clause 1 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

199 Bulk personal datasets: interpretation

(1) For the purposes of this Part **and Part 7A**, an intelligence service retains a bulk personal dataset if—

(a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals,

(b) 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,

(c) after any initial examination of the contents, the intelligence service retains the set for the purpose of the exercise of its functions, and

(d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.

(2) In this Part **and Part 7A**, "personal data" means—

(a) personal data within the meaning of section 3(2) of the Data Protection Act 2018 which is subject to processing described in section 82(1) of that Act, and

(b) data relating to a deceased individual where the data would fall within paragraph (a) if it related to a living individual.

*Requirement for ~~warrant~~ **authorisation***

200 Requirement for authorisation ~~by warrant~~: general

(1) An intelligence service may not exercise a power to retain a bulk personal dataset unless the retention of the dataset is authorised—

(a) by a warrant under this Part**, or**

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

(2) An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised –

(a) by a warrant under this Part**, or**

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

(3) For the purposes of this Part, there are two kinds of warrant—

(a) a warrant, referred to in this Part as "a class BPD warrant", authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset of a class described in the warrant;

(b) a warrant, referred to in this Part as "a specific BPD warrant", authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset described in the warrant.

(4) Section 201 sets out exceptions to the restrictions imposed by subsections (1) and (2) of this section.

201 Exceptions to section 200(1) and (2)

(1) Section 200(1) or (2) does not apply to the exercise of a power of an intelligence service to retain or (as the case may be) examine a bulk personal dataset if the intelligence service obtained the bulk personal dataset under a warrant or other authorisation issued or given under this Act.

(2) Section 200(1) or (2) does not apply at any time when a bulk personal dataset is being retained or (as the case may be) examined for the purpose of enabling any of the information contained in it to be destroyed.

(3) Sections 210(8), 219(8) ~~**and 220(5)**~~ **, 220(5) and 96) and 226CC(3)** provide for other exceptions to section 200(1) or (2) (in connection with cases where a Judicial Commissioner refuses to approve a specific BPD warrant, the non-renewal or cancellation of BPD warrants **or authorisations under Part 7A** and initial examinations).

Restriction on use of class BPD warrants etc

202 Restriction on use of class BPD warrants

(1) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service, or a person acting on their behalf, considers that the bulk personal dataset consists of, or includes, protected data.

For the meaning of "protected data", see section 203.

(2) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service, or a person acting on their behalf, considers—

(a) that the bulk personal dataset consists of, or includes, health records, or

(b) that a substantial proportion of the bulk personal dataset consists of sensitive personal data.

(3) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service, or a person acting on their behalf, considers that the nature of the bulk personal dataset, or the circumstances in

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

(4) In subsection (2)—

"health records" has the same meaning as in section 206;

"sensitive personal data" means personal data consisting of information about an individual (whether living or deceased) which is of a kind mentioned in [section 86(7)(a) to (e) of the Data Protection Act 2018.

(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.

…

220 Initial examinations: time limits

(1) This section applies where—

(a) an intelligence service obtains a set of information otherwise than in the exercise of a power conferred by a warrant or other authorisation issued or given under this Act, and

(b) 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, must take the following steps before the end of the permitted period.

Step 1

Carry out an initial examination of the set for the purpose of deciding whether, if the intelligence service were to retain it after that initial examination and hold it electronically for analysis for the purposes of the exercise of its functions, the intelligence service would be retaining a bulk personal dataset (see section 199).

Step 2

If the intelligence service would be retaining a bulk personal dataset as mentioned in step 1, decide whether to retain the set and hold it electronically for analysis for the purposes of the exercise of the functions of the intelligence service.

~~*Step 3*~~

~~If the head of the intelligence service decides to retain the set and hold it electronically for analysis as mentioned in step 2, apply for a specific BPD warrant as soon as reasonably practicable after making that decision (unless the retention of the dataset is authorised by a class BPD warrant).~~

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.

(3) The permitted period begins when the head of the intelligence service, or a person acting on their behalf, first forms the beliefs mentioned in subsection (1)(b).

(4) The permitted period ends—

(a) where the set of information was created in the United Kingdom, 3 months after the day on which it begins;

(b) where the set of information was created outside the United Kingdom, 6 months after the day on which it begins.

(5) If the head of the intelligence service, or a person acting on their behalf, applies for a specific BPD warrant 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 the period between the taking of the decision mentioned in step 2 and the determination of the application for the specific BPD warrant, 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 for the purposes of the making of the application for the warrant.

(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.

(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.

…

225 Application of Part to bulk personal datasets obtained under this Act

(1) Subject to subsection (2), this section applies where a bulk personal dataset has been obtained by an intelligence service under a warrant or other authorisation issued or given under this Act (and, accordingly, section 200(1) and (2) do not apply by virtue of section 201(1)).

(2) This section does not apply where the bulk personal dataset was obtained by the intelligence service under a bulk acquisition warrant issued under Chapter 2 of Part 6.

(3) Where this section applies, the Secretary of State may, on the application of the head of the intelligence service, or a person acting on their behalf, give a direction that—

(a) the intelligence service may retain, or retain and examine, the bulk personal dataset by virtue of the direction,

(b) any other power of the intelligence service to retain or examine the bulk personal dataset, and any associated regulatory provision, ceases to apply in relation to the bulk personal dataset (subject to subsection (5)), and (c) section 201(1) also ceases to apply in relation to the bulk personal dataset.

(4) Accordingly, where a direction is given under subsection (3), the intelligence service may exercise its power by virtue of the direction to retain, or to retain and examine, the bulk personal dataset only if authorised to do so—

(a) by a class BPD warrant or a specific BPD warrant under this Part**, or**

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

(5) A direction under subsection (3) may provide for any associated regulatory provision specified in the direction to continue to apply in relation to the bulk personal dataset, with or without modifications specified in the direction.

(6) The power conferred by subsection (5) must be exercised to ensure that—

(a) where section 56 and Schedule 3 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to it (without modification);

(b) where sections 57 to 59 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to

it with the modification that the reference in section 58(7)(a) to the provisions of Part 2 is to be read as including a reference to the provisions of this Part.

(7) The Secretary of State may only give a direction under subsection (3) with the approval of a Judicial Commissioner.

(8) In deciding whether to give approval for the purposes of subsection (7), the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(9) Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to give a direction under subsection (3), the Judicial Commissioner must give the Secretary of State written reasons for the decision.

(10) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

(11) A direction under subsection (3)—

(a) may not be revoked;

(b) may be varied but only for the purpose of altering or removing any provision included in the direction under subsection (5).

(12) Subsections (7) to (10) apply in relation to the variation of a direction under subsection (3) as they apply in relation to the giving of a direction under that subsection.

(13) The head of an intelligence service, or a person acting on their behalf, may, at the same time as applying for a direction under subsection (3) apply—

(a) for a specific BPD warrant under section 205 (and the Secretary of State may issue such a warrant at the same time as giving the direction)**, or**

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

(14) In this section, "associated regulatory provision", in relation to a power of an intelligence service to retain or examine a bulk personal dataset, means any provision which—

(a) is made by or for the purposes of this Act (other than this Part), and

(b) applied in relation to the retention, examination, disclosure or other use of the bulk personal dataset immediately before the giving of a direction under subsection (3).

(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.

Clause 3

Duration, modification and cancellation

213 Duration of warrants

(1) A class BPD warrant or a specific BPD warrant ceases to have effect at the end of the relevant period (see subsection (2)) unless—

(a) it is renewed before the end of that period (see section 214), or

(b) it is cancelled or (in the case of a specific BPD warrant) otherwise ceases to have effect before the end of that period (see sections 209 and 218).

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

(a) in the case of an urgent specific BPD warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of ~~6 months~~ **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 subsection (2)(a), a specific BPD warrant is an "urgent specific 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.

(4) For provision about the renewal of warrants, see section 214.

Clause 4

To note: amendments that are made by clause 4 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

Restriction on use of class BPD warrants etc

202 Restriction on use of class BPD warrants

(1) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service**, or a person acting on their behalf,** considers that the bulk personal dataset consists of, or includes, protected data.

For the meaning of "protected data", see section 203.

(2) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service**, or a person acting on their behalf,** considers—

(a) that the bulk personal dataset consists of, or includes, health records, or

(b) that a substantial proportion of the bulk personal dataset consists of sensitive personal data.

(3) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service**, or a person acting on their behalf,** considers that the nature of the bulk personal dataset, or the circumstances in which it was created, is or are such that its retention, or retention and examination, by the intelligence service raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application **~~by the head of the intelligence service~~** for a specific BPD warrant.

(4) In subsection (2)—

"health records" has the same meaning as in section 206;

"sensitive personal data" means personal data consisting of information about an individual (whether living or deceased) which is of a kind mentioned in [section 86(7)(a) to (e) of the Data Protection Act 2018.

(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.

…

206 Additional safeguards for health records

(1) Subsections (2) and (3) apply if—

(a) an application is made by or on behalf of the head of an intelligence service for the issue of a specific BPD warrant, and

(b) the purpose, or one of the purposes, of the warrant is to authorise the retention, or the retention and examination, of health records.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to authorise the retention, or the retention and examination, of health records.

(3) The Secretary of State may issue the warrant only if the Secretary of State considers that there are exceptional and compelling circumstances that make it necessary to authorise the retention, or the retention and examination, of health records.

(4) Subsection (5) applies if—

(a) an application is made by or on behalf of the head of an intelligence service for a specific BPD warrant,

(b) the head of the intelligence service**, or a person acting on their behalf,** considers that the bulk personal dataset includes, or is likely to include, health records, and

(c) subsections (2) and (3) do not apply.

(5) The application must contain either—

(a) a statement that the head of the intelligence service**, or a person acting on their behalf,** considers that the bulk personal dataset includes health records, or

(b) a statement that the head of the intelligence service**, or a person acting on their behalf,** considers that it is likely that the bulk personal dataset includes health records and an assessment of how likely this is.

(6) 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 intelligence service 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.

(7) In subsection (6)—

"health professional" has the same meaning as in the Data Protection Act 2018 (see section 204(1) of that Act);

"health service body" has meaning given by section 204(4) of that Act.

(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.

…

219 Non-renewal or cancellation of BPD warrants

(1) This section applies where a class BPD warrant or a specific 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**, 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 warrant ceases to have effect—

(a) apply for—

(i) a specific BPD warrant authorising the retention, or the retention and examination, of the whole or any part of the material retained by the intelligence service in reliance on the warrant which has ceased to have effect;

(ii) a class BPD warrant authorising the retention or (as the case may be) the retention and examination of bulk personal datasets of a class that is described in a way that would authorise the retention or (as the case may be) the retention and examination of the whole or any part of such material, or

(b) where the head of the intelligence service**, or a person acting on their behalf,** wishes to give further consideration to whether to apply for a warrant of a kind mentioned in paragraph (a)(i) or (ii), apply to the Secretary of State for authorisation to retain, or to retain and examine, the whole or any part of the material retained by the intelligence service in reliance on the warrant.

(3) On an application under subsection (2)(b), the Secretary of State may—

(a) direct that any of the material to which the application relates be destroyed;

(b) with the approval of a Judicial Commissioner, authorise the retention or (as the case may be) the retention and examination of any of that material, subject to such conditions as the Secretary of State considers appropriate, for a period specified by the Secretary of State which may not exceed 3 months.

(4) In deciding whether to give approval for the purposes of subsection (3)(b), 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).

(5) Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to authorise the retention or (as the case may be) the retention and examination of any

material under subsection (3)(b), the Judicial Commissioner must give the Secretary of State written reasons for the decision.

(6) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

(7) If, during the period specified by the Secretary of State under subsection (3)(b), the head of the intelligence service**, or a person acting on their behalf,** decides to apply for a warrant of a kind mentioned in subsection (2)(a)(i) or (ii), the head of the intelligence service**, or a person acting on their behalf,** must make the application as soon as reasonably practicable and before the end of the period specified by the Secretary of State.

(8) Where a class BPD warrant or a specific BPD warrant ceases to have effect because it expires without having been renewed or 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 warrant related during any of the following periods.

First period

The period of 5 working days beginning with the day on which the warrant ceases to have effect.

Second period

The period beginning with the day on which the head of the intelligence service**, or a person acting on their behalf,** makes an application under subsection (2)(a) or (b) in relation to the material and ending with the determination of the application.

Third period

The period during which the retention or examination of the material is authorised under subsection (3)(b).

Fourth period

Where authorisation under subsection (3)(b) is given and the head of the intelligence service**, or a person acting on their behalf,** subsequently makes, in accordance with subsection (7), an application for a specific BPD warrant or a class BPD warrant in relation to the material, the period (if any) beginning with the expiry of the authorisation under subsection (3)(b) and ending with the determination of the application for the warrant.

(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.

220 Initial examinations: time limits

(1) This section applies where—

(a) an intelligence service obtains a set of information otherwise than in the exercise of a power conferred by a warrant or other authorisation issued or given under this Act, and

(b) 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,** must take the following steps before the end of the permitted period.

Step 1

Carry out an initial examination of the set for the purpose of deciding whether, if the intelligence service were to retain it after that initial examination and hold it electronically for analysis for the purposes of the exercise of its functions, the intelligence service would be retaining a bulk personal dataset (see section 199).

Step 2

If the intelligence service would be retaining a bulk personal dataset as mentioned in step 1, decide whether to retain the set and hold it electronically for analysis for the purposes of the exercise of the functions of the intelligence service.

~~*Step 3*~~

~~If the head of the intelligence service decides to retain the set and hold it electronically for analysis as mentioned in step 2, apply for a specific BPD warrant as soon as reasonably practicable after making that decision (unless the retention of the dataset is authorised by a class BPD warrant).~~

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.

(3) The permitted period begins when the head of the intelligence service**, or a person acting on their behalf,** first forms the beliefs mentioned in subsection (1)(b).

(4) The permitted period ends—

(a) where the set of information was created in the United Kingdom, 3 months after the day on which it begins;

(b) where the set of information was created outside the United Kingdom, 6 months after the day on which it begins.

(5) If the head of the intelligence service**, or a person acting on their behalf,** applies for a specific BPD warrant 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 the period between the taking of the decision mentioned in step 2 and the determination of the application for the specific BPD warrant, 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 for the purposes of the making of the application for the warrant.

(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.

(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.

…

225 Application of Part to bulk personal datasets obtained under this Act

(1) Subject to subsection (2), this section applies where a bulk personal dataset has been obtained by an intelligence service under a warrant or other authorisation issued or given under this Act (and, accordingly, section 200(1) and (2) do not apply by virtue of section 201(1)).

(2) This section does not apply where the bulk personal dataset was obtained by the intelligence service under a bulk acquisition warrant issued under Chapter 2 of Part 6.

(3) Where this section applies, the Secretary of State may, on the application of the head of the intelligence service**, or a person acting on their behalf**, give a direction that—

(a) the intelligence service may retain, or retain and examine, the bulk personal dataset by virtue of the direction,

(b) any other power of the intelligence service to retain or examine the bulk personal dataset, and any associated regulatory provision, ceases to apply in relation

to the bulk personal dataset (subject to subsection (5)), and (c) section 201(1) also ceases to apply in relation to the bulk personal dataset.

(4) Accordingly, where a direction is given under subsection (3), the intelligence service may exercise its power by virtue of the direction to retain, or to retain and examine, the bulk personal dataset only if authorised to do so—

(a) by a class BPD warrant or a specific BPD warrant under this Part, or

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

(5) A direction under subsection (3) may provide for any associated regulatory provision specified in the direction to continue to apply in relation to the bulk personal dataset, with or without modifications specified in the direction.

(6) The power conferred by subsection (5) must be exercised to ensure that—

(a) where section 56 and Schedule 3 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to it (without modification);

(b) where sections 57 to 59 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to it with the modification that the reference in section 58(7)(a) to the provisions of Part 2 is to be read as including a reference to the provisions of this Part.

(7) The Secretary of State may only give a direction under subsection (3) with the approval of a Judicial Commissioner.

(8) In deciding whether to give approval for the purposes of subsection (7), the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(9) Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to give a direction under subsection (3), the Judicial Commissioner must give the Secretary of State written reasons for the decision.

(10) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

(11) A direction under subsection (3)—

(a) may not be revoked;

(b) may be varied but only for the purpose of altering or removing any provision included in the direction under subsection (5).

(12) Subsections (7) to (10) apply in relation to the variation of a direction under subsection (3) as they apply in relation to the giving of a direction under that subsection.

(13) The head of an intelligence service**, or a person acting on their behalf,** may, at the same time as applying for a direction under subsection (3) apply—

(a) for a specific BPD warrant under section 205 (and the Secretary of State may issue such a warrant at the same time as giving the direction), or

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

(14) In this section, "associated regulatory provision", in relation to a power of an intelligence service to retain or examine a bulk personal dataset, means any provision which—

(a) is made by or for the purposes of this Act (other than this Part), and

(b) applied in relation to the retention, examination, disclosure or other use of the bulk personal dataset immediately before the giving of a direction under subsection (3).

(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.

Clause 6

Overview and general privacy duties

1 Overview of Act

(1) This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.

(2) This Part imposes certain duties in relation to privacy and contains other protections for privacy.

(3) These other protections include offences and penalties in relation to—

(a) the unlawful interception of communications, and

(b) the unlawful obtaining of communications data.

(4) This Part also abolishes and restricts various general powers to obtain communications data and restricts the circumstances in which equipment interference, and certain requests about the interception of communications, can take place.

(5) Further protections for privacy—

(a) can be found, in particular, in the regimes provided for by Parts 2 to 7 and in the oversight arrangements in Part 8, and

(b) also exist—

(i) by virtue of the Human Rights Act 1998,

(ii) in section 170 of the Data Protection Act 2018 (unlawful obtaining etc of personal data),

(iii) in section 48 of the Wireless Telegraphy Act 2006 (offence of interception or disclosure of messages),

(iv) in sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences),

(v) in the common law offence of misconduct in public office, and

(vi) elsewhere in the law.

(6) The regimes provided for by ~~**Parts 2 to 7**~~ **Parts 2 to 7B** are as follows—

(a) Part 2 and Chapter 1 of Part 6 set out circumstances (including under a warrant) in which the interception of communications is lawful and make further provision about the interception of communications and the treatment of material obtained in connection with it,

(b) Part 3 and Chapter 2 of Part 6 set out circumstances in which the obtaining of communications data is lawful in pursuance of an authorisation or under a warrant and make further provision about the obtaining and treatment of such data,

(c) Part 4 makes provision for the retention of certain communications data in pursuance of a notice,

(d) Part 5 and Chapter 3 of Part 6 deal with equipment interference warrants, and

(e) ~~**Part 7 deals**~~ **Parts 7 to 7B deal** with bulk personal dataset warrants **and authorisations**.

(7) As to the rest of the Act—

(a) Part 8 deals with oversight arrangements for regimes in this Act and elsewhere, and

(b) Part 9 contains miscellaneous and general provisions including amendments to sections 3 and 5 of the Intelligence Services Act 1994 and provisions about national security and combined warrants and authorisations.

2 General duties in relation to privacy

(1) Subsection (2) applies where a public authority is deciding whether—

(a) to issue, renew or cancel a warrant under Part 2, 5, 6 ~~**or 7**~~ **7 or 7B**,

(b) to modify such a warrant,

(c) to approve a decision to issue, renew or modify such a warrant,

(d) to grant, approve or cancel an authorisation under Part 3,

(e) to give a notice in pursuance of such an authorisation or under Part 4 or section 252, 253 or 257,

(f) to vary or revoke such a notice,

(g) to approve a decision to give or vary a notice under Part 4 or section 252, 253 or 257,

(h) to approve the use of criteria under section 153, 194 or 222,

(i) to give an authorisation under section 219(3)(b),

(j) to approve a decision to give such an authorisation, ~~**or**~~

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

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

(k) to apply for or otherwise seek any issue, grant, giving, modification, variation or renewal of a kind falling within paragraph (a), (b), (d), (e), (f) ~~**or (i), (i) or (ja)**~~.

(2) The public authority must have regard to—

(a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,

(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,

(c) the public interest in the integrity and security of telecommunication systems and postal services, and

(d) any other aspects of the public interest in the protection of privacy.

(3) The duties under subsection (2)—

(a) apply so far as they are relevant in the particular context, and

(b) are subject to the need to have regard to other considerations that are also relevant in that context.

(4) The other considerations may, in particular, include—

(a) the interests of national security or of the economic well-being of the United Kingdom,

(b) the public interest in preventing or detecting serious crime,

(c) other considerations which are relevant to—

(i) whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or

(ii) whether it is necessary to act for a purpose provided for by this Act,

(d) the requirements of the Human Rights Act 1998, and

(e) other requirements of public law.

(5) For the purposes of subsection (2)(b), examples of sensitive information include—

(a) items subject to legal privilege,

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

(c) relevant confidential information within the meaning given by paragraph 2(4) of Schedule 7 (certain information held in confidence and consisting of personal records, journalistic material or communications between Members of Parliament and their constituents).

(6) […]

Clause 7

To note: amendments that are made by clause 7 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

The Commissioners

227 Investigatory Powers Commissioner and other Judicial Commissioners

(1) The Prime Minister must appoint—

(a) the Investigatory Powers Commissioner, and

(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

(2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

(3) A person is not to be appointed as the Investigatory Powers Commissioner unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session, and

(d) the Lord Chief Justice of Northern Ireland.

(4) A person is not to be appointed as a Judicial Commissioner under subsection (1)(b) unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session,

(d) the Lord Chief Justice of Northern Ireland, and

(e) the Investigatory Powers Commissioner.

(5) Before appointing any person under subsection (1), the Prime Minister must consult the Scottish Ministers.

(6) The Prime Minister must have regard to a memorandum of understanding agreed between the Prime Minister and the Scottish Ministers when exercising functions under subsection (1) or (5).

(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.

(7) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

~~(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 any other Judicial Commissioner.~~

~~(9) Subsection (8) does not apply to the function of the Investigatory Powers Commissioner of making a recommendation under subsection (4)(e) or making an appointment under section 247(1).~~

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

(c) 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.

~~(9A) Subsection (8) applies to the functions of the Investigatory Powers Commissioner under section 60A or 65(3B) only where the Investigatory Powers Commissioner is unable to exercise the functions because of illness or absence or for any other reason.~~

(10) The delegation under subsection (8) to any extent of functions by the Investigatory Powers Commissioner does not prevent the exercise of the functions to that extent by that Commissioner.

(10A) Where—

(a) the exercise of a function of the Investigatory Powers Commissioner mentioned in subsection (8A)(c) 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.

(11) Any function exercisable by a Judicial Commissioner or any description of Judicial Commissioners is exercisable by any of the Judicial Commissioners or (as the case may be) any of the Judicial Commissioners of that description.

(12) Subsection (11) does not apply to—

(a) any function conferred on the Investigatory Powers Commissioner by name (except so far as its exercise by any of the Judicial Commissioners or any description of Judicial Commissioners is permitted by a delegation under subsection (8)), or

(b) any function conferred on, or delegated under subsection (8) to, any other particular named Judicial Commissioner.

(13) References in any enactment—

(a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and

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

(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.

(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.

228 Terms and conditions of appointment

(1) Subject as follows, each Judicial Commissioner holds and vacates office in accordance with the Commissioner's terms and conditions of appointment.

(2) Each Judicial Commissioner is to be appointed for a term of three years.

(3) A person who ceases to be a Judicial Commissioner (otherwise than under subsection (5)) may be re-appointed under section 227(1).

(4) A Judicial Commissioner may not, subject to subsection (5), be removed from office before the end of the term for which the Commissioner is appointed unless a resolution approving the removal has been passed by each House of Parliament.

(5) A Judicial Commissioner may be removed from office by the Prime Minister if, after the appointment of the Commissioner—

(a) a bankruptcy order is made against the Commissioner or the Commissioner's estate is sequestrated or the Commissioner makes a composition or arrangement with, or grants a trust deed for, the Commissioner's creditors,

(b) any of the following orders is made against the Commissioner—

(i) a disqualification order under the Company Directors Disqualification Act 1986 or the Company Directors Disqualification (Northern Ireland) Order 2002,

(ii) an order under section 429(2)(b) of the Insolvency Act 1986 (failure to pay under county court administration order),

(iii) an order under section 429(2) of the Insolvency Act 1986 (disabilities on revocation of county court administration order),

(c) the Commissioner's disqualification undertaking is accepted under section 7 or 8 of the Company Directors Disqualification Act 1986 or under the Company Directors Disqualification (Northern Ireland) Order 2002, or

(d) the Commissioner is convicted in the United Kingdom, the Channel Islands or the Isle of Man of an offence and receives a sentence of imprisonment (whether suspended or not).

(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.

…

263 General definitions

(1) In this Act—

"apparatus" includes any equipment, machinery or device (whether physical or logical) and any wire or cable,

"civil proceedings" means any proceedings in or before any court or tribunal that are not criminal proceedings,

"crime" means conduct which—

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences,

"criminal proceedings" includes proceedings before a court in respect of a service offence within the meaning of the Armed Forces Act 2006 (and references to criminal prosecutions are to be read accordingly),

"data" includes data which is not electronic data and any information (whether or not electronic),

"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)),

"destroy", in relation to electronic data, means delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly),

…

…

265 Index of defined expressions

In this Act, the expressions listed in the left-hand column have the meaning given by, or are to be interpreted in accordance with, the provisions listed in the right-hand column.

Expression	*Provision*
…	…
Data	Section 263(1)
Deputy Investigatory Powers Commissioner	**Section 263(1)**
Destroy (in relation to electronic data) and related expressions	Section 263(1)
…	…

Clause 8

To note: amendments that are made by clause 8 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

The Commissioners

227 Investigatory Powers Commissioner and other Judicial Commissioners

(1) The Prime Minister must appoint—

(a) the Investigatory Powers Commissioner, and

(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

(2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

(3) A person is not to be appointed as the Investigatory Powers Commissioner unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session, and

(d) the Lord Chief Justice of Northern Ireland.

(4) A person is not to be appointed as a Judicial Commissioner under subsection (1)(b) unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session,

(d) the Lord Chief Justice of Northern Ireland, and

(e) the Investigatory Powers Commissioner.

(5) Before appointing any person under subsection (1), the Prime Minister must consult the Scottish Ministers.

(6) The Prime Minister must have regard to a memorandum of understanding agreed between the Prime Minister and the Scottish Ministers when exercising functions under subsection (1) or (5).

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

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

(7) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

~~**(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 any other Judicial Commissioner.**~~

~~**(9) Subsection (8) does not apply to the function of the Investigatory Powers Commissioner of making a recommendation under subsection (4)(e) or making an appointment under section 247(1).**~~

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

(c) 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.

~~**(9A) Subsection (8) applies to the functions of the Investigatory Powers Commissioner under section 60A or 65(3B) only where the Investigatory Powers Commissioner is unable to exercise the functions because of illness or absence or for any other reason.**~~

(10) The delegation under subsection (8) to any extent of functions by the Investigatory Powers Commissioner does not prevent the exercise of the functions to that extent by that Commissioner.

(10A) Where—

(a) the exercise of a function of the Investigatory Powers Commissioner mentioned in subsection (8A)(c) 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.

(11) Any function exercisable by a Judicial Commissioner or any description of Judicial Commissioners is exercisable by any of the Judicial Commissioners or (as the case may be) any of the Judicial Commissioners of that description.

(12) Subsection (11) does not apply to—

(a) any function conferred on the Investigatory Powers Commissioner by name (except so far as its exercise by any of the Judicial Commissioners or any description of Judicial Commissioners is permitted by a delegation under subsection (8)), or

(b) any function conferred on, or delegated under subsection (8) to, any other particular named Judicial Commissioner.

(13) References in any enactment—

(a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and

~~**(b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (8), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner.**~~

(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.

(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.

…

238 Funding, staff and facilities etc.

(1) There is to be paid to the Judicial Commissioners out of money provided by Parliament such remuneration and allowances as the Treasury may determine.

(2) The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

(a) such staff, and

(b) such accommodation, equipment and other facilities and services,

as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.

(3) The Scottish Ministers may pay to the Judicial Commissioners such allowances as the Scottish Ministers consider appropriate in respect of the exercise by the Commissioners of functions which relate to the exercise by Scottish public authorities of devolved functions.

(4) In subsection (3)—

"devolved function" means a function that does not relate to reserved matters (within the meaning of the Scotland Act 1998), and

"Scottish public authority" has the same meaning as in the Scotland Act 1998.

(5) The Investigatory Powers Commissioner or any other Judicial Commissioner may, to such extent as the Commissioner concerned may decide, delegate the exercise of functions of that Commissioner to any member of staff of the Judicial Commissioners or any other person acting on behalf of the Commissioners.

(6) Subsection (5) does not apply to—

(a) the function of the Investigatory Powers Commissioner of making a recommendation under section 227(4)(e) or making an appointment under section **227(6A), 228A(2) or** 247(1),

(b) any function which falls within section 229(8), or

(c) any function under section 58(4) or 133(3) of authorising a disclosure,

but, subject to this and the terms of the delegation, does include functions which have been delegated to a Judicial Commissioner by the Investigatory Powers Commissioner.

(7) The delegation under subsection (5) to any extent of functions by the Investigatory Powers Commissioner or any other Judicial Commissioner does not prevent the exercise of the functions to that extent by the Commissioner concerned.

Clause 10

229 Main oversight functions

(1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to—

(a) the interception of communications,

(b) the acquisition or retention of communications data,

(c) the obtaining of related communications data under Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000,

(d) equipment interference.

(2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of—

(a) any content of communications intercepted by an interception authorised or required by a warrant under Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000,

(b) acquired or retained communications data,

(c) data acquired as mentioned in subsection (1)(c), or

(d) communications, equipment data or other information acquired by means of equipment interference.

(3) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation)—

(a) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service,

(b) the giving and operation of notices under section 252 (national security notices),

~~**(c) the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc.),**~~

(d) the exercise of functions by virtue of sections 1 to 4 of the Prisons (Interference with Wireless Telegraphy) Act 2012,

(e) the exercise of functions by virtue of Part 2 or 3 of the Regulation of Investigatory Powers Act 2000 (surveillance, covert human intelligence sources and investigation of electronic data protected by encryption etc.),

(f) the adequacy of the arrangements by virtue of which the duties imposed by section 55 of that Act are sought to be discharged,

(g) the exercise of functions by virtue of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (surveillance and covert human intelligence sources),

(h) the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property),

(i) the exercise by the Secretary of State of functions under sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property etc.), and

(j) the exercise by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998) of functions under sections 5 and 6(3) and (4) of the Act of 1994.

(3A) The Investigatory Powers Commissioner must, in accordance with the Agreement between the Government of the United Kingdom and the Government of the United States of America on access to electronic data for the purpose of countering serious crime dated 3rd October 2019, keep under review the compliance by public authorities with the terms of that Agreement.

(3B) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the process operated by GCHQ for determining whether information about vulnerabilities in technology should be disclosed.

(3C) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) compliance by the persons mentioned in subsection (3D) with "The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees", as published on 18th July 2019.

(3D) Those persons are—

(a) members and civilian staff of the metropolitan police force who are carrying out activities to which a collaboration agreement made under section 22A of the Police Act 19968 relating to counter-terrorism activities applies, and

(b) officers of the National Crime Agency.

(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).

(4) But the Investigatory Powers Commissioner is not to keep under review—

(a) the exercise of any function of a relevant Minister to make subordinate legislation,

(b) the exercise of any function by a judicial authority,

(c) the exercise of any function by virtue of Part 3 of the Regulation of Investigatory Powers Act 2000 which is exercisable with the permission of a judicial authority,

(d) the exercise of any function which—

(i) is for the purpose of obtaining information or taking possession of any document or other property in connection with communications stored in or by a telecommunication system, or

(ii) is carried out in accordance with an order made by a judicial authority for that purpose,

and is not exercisable by virtue of this Act, the Regulation of Investigatory Powers Act 2000, the Regulation of Investigatory Powers (Scotland) Act 2000, the Crime (Overseas Production Orders) Act 2019 or an enactment mentioned in subsection (3)(c), (h), (i) or (j) above,

(e) the exercise of any function where the conduct concerned is—

(i) conduct authorised by section 45, 47 or 50, or

(ii) conduct authorised by section 46 which is not conduct by or on behalf of an intercepting authority (within the meaning given by section 18(1)), or

(f) the exercise of any function which is subject to review by the Information Commissioner or the Investigatory Powers Commissioner for Northern Ireland.

(4A) In keeping matters under review in accordance with subsection (3)(e), the Investigatory Powers Commissioner must, in particular, keep under review the exercise of the power to grant or renew authorisations under section 29B of the Regulation of Investigatory Powers Act 2000.

(4B) In keeping under review the exercise of the power mentioned in subsection (4A), the Investigatory Powers Commissioner must, in particular, keep under review whether public authorities are complying with any requirements imposed on them by virtue of Part 2 of the Regulation of Investigatory Powers Act 2000 in relation to juvenile criminal conduct authorisations and vulnerable adult criminal conduct authorisations.

(4C) For the purposes of subsection (4B)—

(a) "a juvenile criminal conduct authorisation" is an authorisation under section 29B of the Regulation of Investigatory Powers Act 2000 where the covert human intelligence source to whom the authorisation relates is under the age of 18; and

(b) "a vulnerable adult criminal conduct authorisation" is an authorisation under section 29B of the Regulation of Investigatory Powers Act 2000 where the covert human intelligence source to whom the authorisation relates is a vulnerable adult within the meaning of section 29D(3) of that Act.

(5) In keeping matters under review in accordance with this section, the Investigatory Powers Commissioner must, in particular, keep under review the operation of safeguards to protect privacy.

(6) In exercising functions under this Act, a Judicial Commissioner must not act in a way which the Commissioner considers to be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime, or

(c) the economic well-being of the United Kingdom.

(7) A Judicial Commissioner must, in particular, ensure that the Commissioner does not—

(a) jeopardise the success of an intelligence or security operation or a law enforcement operation,

(b) compromise the safety or security of those involved, or

(c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.

(8) Subsections (6) and (7) do not apply in relation to any of the following functions of a Judicial Commissioner—

(a) deciding—

(i) whether to serve, vary or cancel a monetary penalty notice under section 1(1A)12 of, or paragraph 11 of Schedule A113 to, the Regulation of Investigatory Powers Act 2000, a notice of intent under paragraph 3 of that Schedule or an information notice under paragraph 9 of that Schedule, or

(ii) the contents of any such notice,

(b) deciding whether to approve the issue, modification or renewal of a warrant,

(c) deciding whether to direct the destruction of material or how otherwise to deal with the situation where—

(i) a warrant issued, or modification made, for what was considered to be an urgent need is not approved, or

(ii) an item subject to legal privilege is retained, following its examination, for purposes other than the destruction of the item,

(d) deciding whether to—

(i) approve the grant, modification or renewal of an authorisation, or

(ii) quash or cancel an authorisation or renewal,

(e) deciding whether to approve—

(i) the giving or varying of a retention notice under Part 4 or a notice under section 252 or 253, or

(ii) the giving of a notice under section 90(10)(b) or 257(9)(b),

(f) participating in a review under section 90 or 257,

(g) deciding whether to approve an authorisation under section 219(3)(b),

(h) deciding whether to give approval under section 222(4),

(i) deciding whether to approve the giving or varying of a direction under section 225(3),

(j) making a decision under section 231(1),

(k) deciding whether to order the destruction of records under section 103 of the Police Act 1997, section 37 of the Regulation of Investigatory Powers Act 2000 or section 15 of the Regulation of Investigatory Powers (Scotland) Act 2000,

(l) deciding whether to make an order under section 103(6) of the Police Act 1997 (order enabling the taking of action to retrieve anything left on property in pursuance of an authorisation),

(m) deciding—

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

(ii) any action to take as a result.

(8A) Subsections (6) and (7) also do not apply in relation to the functions of the Investigatory Powers Commissioner under section 60A or 65(3B).

(9) In this section—

"bulk personal dataset" is to be read in accordance with section 199,

"equipment data" has the same meaning as in Part 5 (see section 100),

"judicial authority" means a judge, court or tribunal or any person exercising the functions of a judge, court or tribunal (but does not include a Judicial Commissioner),

"police force" has the same meaning as in Part 2 (see section 60(1)),

"related systems data" has the meaning given by section 15(6),

"relevant Minister" means a Minister of the Crown or government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department,

"secondary data" has the same meaning as in Part 2 (see section 16).

230 Additional directed oversight functions

(1) So far as directed to do so by the Prime Minister and subject to subsection (2), the Investigatory Powers Commissioner must keep under review the carrying out of any aspect of the functions of—

(a) an intelligence service,

(b) a head of an intelligence service, **~~or~~**

(c) any part of Her Majesty's forces, or of the Ministry of Defence, so far as engaging in intelligence activities**, 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.

(2) Subsection (1) does not apply in relation to anything which is required to be kept under review by the Investigatory Powers Commissioner under section 229.

(3) The Prime Minister may give a direction under this section at the request of the Investigatory Powers Commissioner or the Intelligence and Security Committee of Parliament or otherwise.

(4) The Prime Minister must publish, in a manner which the Prime Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Prime Minister that such publication would be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

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

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

231 Error reporting

(1) The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that—

(a) the error is a serious error, and

(b) it is in the public interest for the person to be informed of the error.

(2) In making a decision under subsection (1)(a), the Investigatory Powers Commissioner may not decide that an error is a serious error unless the Commissioner considers that the error has caused significant prejudice or harm to the person concerned.

(3) Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

(4) In making a decision under subsection (1)(b), the Investigatory Powers Commissioner must, in particular, consider—

(a) the seriousness of the error and its effect on the person concerned, and

(b) the extent to which disclosing the error 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.

(5) Before making a decision under subsection (1)(a) or (b), the Investigatory Powers Commissioner must ask the public authority which has made the error to make submissions to the Commissioner about the matters concerned.

(6) When informing a person under subsection (1) of an error, the Investigatory Powers Commissioner must—

(a) inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and

(b) provide such details of the error 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 (4)(b)(i) to (iv).

(7) The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section.

(8) A report under section 234(1) must include information about—

(a) the number of relevant errors of which the Investigatory Powers Commissioner has become aware during the year to which the report relates,

(b) the number of relevant errors which the Commissioner has decided during that year were serious errors, and

(c) the number of persons informed under subsection (1) during that year.

(9) In this section "relevant error" means an error—

(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and

(b) of a description identified for this purpose in a **~~code of practice under Schedule 7~~ relevant code of practice**,

and the Investigatory Powers Commissioner must keep under review the definition of "relevant error".

(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.

Clause 11

6 Definition of "lawful authority" <u>in relation to interceptions</u>

(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with—

(i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(ii) a bulk interception warrant under Chapter 1 of Part 6,

(b) the interception is authorised by any of sections 44 to 52, or

(c) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is carried out in accordance with a targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6,

(ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or

(iii) is carried out in accordance with a court order made for that purpose.

(2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.

(3) Any other conduct which—

(a) is carried out in accordance with a warrant under Chapter 1 of Part 2 or a bulk interception warrant, or

(b) is authorised by any of sections 44 to 52, is to be treated as lawful for all purposes.

…

11 Offence of unlawfully obtaining communications data

(1) A relevant person who, without lawful authority, knowingly or recklessly obtains communications data **~~from a telecommunications operator or a postal operator is guilty of an offence~~** **<u>from—</u>**

<u>(a) a telecommunications operator which is not a public authority, or</u>

<u>(b) a postal operator,</u>

is guilty of an offence.

(2) In this section "relevant person" means a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

(3) Subsection (1) does not apply to a relevant person who shows that the person acted in the reasonable belief that the person had lawful authority to obtain the communications data.

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

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding the general limit in a magistrates' court (or 6 months, if the offence was committed before 2 May 2022), or

(ii) to a fine, or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum, or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) 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 or to a fine, or to both.

Clause 12

261 Telecommunications definitions

…

Communications data

(5) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but **(subject to subsection (5A))** does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.

(5A) In subsection (5) the words after paragraph (c) do not apply to entity data which is about an entity to which a telecommunications service is provided and—

(a) may be used to identify, or assist in identifying, that entity, or

(b) may be used to identify, or assist in identifying, the location of that entity.

…

Clause 13

12 Abolition or restriction of certain powers to obtain communications data

(1) Schedule 2 (which repeals certain information powers so far as they enable public authorities to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator) has effect.

(2) Any general information power which—

(a) would (apart from this subsection) enable a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator, and

(b) does not involve a court order or other judicial authorisation or warrant **~~and is not a regulatory power or a relevant postal power~~**,

is to be read as not enabling the public authority to secure such a disclosure.

(2A) Subsection (2) is subject to section 352(1) of the Finance (No. 2) Act 2023 (no restriction on tax related powers) **and subsection (2B)**.

(2B) Subsection (2) does not apply to the exercise, 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.

~~(3) A regulatory power or relevant postal power which enables a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator may only be exercised by the public authority for that purpose if it is not possible for the authority to use a power under this Act to secure the disclosure of the data.~~

(4) The Secretary of State may by regulations modify any enactment in consequence of subsection (2).

(5) In this section "general information power" means—

(a) in relation to disclosure by a telecommunications operator, any power to obtain information or documents (however expressed) which—

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

(ii) does not deal (whether alone or with other matters) specifically with telecommunications operators or any class of telecommunications operators, and

(b) in relation to disclosure by a postal operator, any power to obtain information or documents (however expressed) which—

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

(ii) does not deal (whether alone or with other matters) specifically with postal operators or any class of postal operators.

(6) In this section—

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

"power" includes part of a power,

~~**"regulatory power" means any power to obtain information or documents (however expressed) 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 the regulation of—**~~

~~**(i) telecommunications operators, telecommunications services or telecommunication systems, or**~~

~~**(ii) postal operators or postal services,**~~

"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 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,

~~**"relevant postal power" means any power to obtain information or documents (however expressed) 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 the conveyance or expected conveyance of any postal item into or out of the United Kingdom,**~~

and references to powers include duties (and references to enabling and exercising are to be read as including references to requiring and performing).

Clause 14

62 Restrictions in relation to internet connection records

(A1) The Investigatory Powers Commissioner may not, on the application of a local authority, grant an authorisation under section 60A for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record.

(A2) The Investigatory Powers Commissioner may not, on the application of a relevant public authority which is not a local authority, grant an authorisation under section 60A for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B **~~or C~~, C or D1** is met.

(1) […]

(2) A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation **under section 61 or 61A** for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B **~~or C~~ , C or D2** is met.

(3) Condition A is that the person with power to grant the authorisation considers that it is necessary, for a purpose falling within section 60A(7), 61(7) or 61A(7) (as applicable), to obtain the data to identify which person or apparatus is using an internet service where—

(a) the service and time of use are already known, but

(b) the identity of the person or apparatus using the service is not known.

(4) Condition B is that—

(a) the purpose for which the data is to be obtained falls within section 60A(7), 61(7) or 61A(7) (as applicable) but is not the purpose of preventing or detecting serious crime mentioned in section 60A(8)(a), 61(7A)(a) or 61A(8)(a) or the purpose of preventing or detecting crime mentioned in section 60A(8)(b), 61(7A)(b) or 61A(8)(b), and

(b) the person with power to grant the authorisation considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) Condition C is that—

(a) either—

(i) the purpose for which the data is to be obtained is the purpose of preventing or detecting serious crime mentioned in section 60A(8)(a), 61(7A)(a) or 61A(8)(a), or

(ii) the purpose for which the data is to be obtained is the purpose of preventing or detecting crime mentioned in section 60A(8)(b), 61(7A)(b) or 61A(8)(b) and the crime to be prevented or detected is serious crime, and

(b) […]

(c) the person with power to grant the authorisation considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(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 28 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.

(6) […]

(7) In this Act "internet connection record" means communications data which—

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

Clause 15

87 Powers to require retention of certain data

…

(4) A retention notice must not require an operator who controls or provides a telecommunication system ("the system operator") to retain data**, other that data which is, or can only be obtained by processing, an internet connection record,** which—

(a) relates to the use of a telecommunications service provided **(solely or jointly with another person)** by another telecommunications operator in relation to that system,

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

(b) is (or is capable of being) processed by the system operator as a result of being comprised in, included as part of, attached to or logically associated with a communication transmitted by means of the system as a result of the use mentioned in paragraph (a),

(c) is not needed by the system operator for the functioning of the system in relation to that communication, and

(d) is not retained or used by the system operator for any other lawful purpose,

and which it is reasonably practicable to separate from other data which is subject to the notice.

(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.

…

(11) In this Part "relevant communications data" means communications data which may be used to identify, or assist in identifying, any of the following—

(a) the sender or recipient of a communication (whether or not a person),

(b) the time or duration of a communication,

(c) the type, method or pattern, or fact, of communication,

(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

(e) the location of any such system,

~~and~~ (and this expression therefore includes, in particular, internet connection **~~records~~ records)**.

Clause 16

To note: amendments that are made by clause 16 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

95 Enforcement of notices and certain other requirements and restrictions

(1) It is the duty of a telecommunications operator on whom a requirement or restriction is imposed by—

(a) a retention notice, or

(b) section 92 or 93,

to comply with the requirement or restriction.

(2) A telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, must not disclose the existence or contents of a retention notice to any other person.

(3) The Information Commissioner, or any member of staff of the Information Commissioner, must not disclose the existence or contents of a retention notice to any other person.

(4) Subsections (2) and (3) do not apply to a disclosure made with the permission of the Secretary of State.

(5) The duty under subsection (1) or (2) or under section 90(4A) is enforceable **(whether or not the person is in the United Kingdom)** 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.

97 Extra-territorial application of Part 4

(1) A retention notice, and any requirement or restriction imposed by virtue of a retention notice or by section 92, 93 or 95(1) to (3), may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

~~**(2) But section 95(5), so far as relating to those requirements or restrictions, does not apply to a person outside the United Kingdom.**~~

Clause 17

To note: amendments that are made by clause 17 are shown in bold and underlined. Amendments made to the same provisions by other clauses of the Bill are underlined.

90 Review by the Secretary of State

(1) A telecommunications operator to whom a retention notice is given may, within such period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State.

(2) Such a reference may be in relation to the whole of a notice or any aspect of it.

(3) In the case of a notice given to a description of operators—

(a) each operator falling within that description may make a reference under subsection (1), but

(b) each such reference may only be in relation to the notice, or aspect of the notice, so far as it applies to that operator.

~~**(4) There is no requirement for an operator who has referred a retention notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (5).**~~

(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.

(5) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).

(6) Before deciding the review, the Secretary of State must consult—

(a) the Technical Advisory Board, and

(b) a Judicial Commissioner.

(7) The Board must consider the technical requirements and the financial consequences, for the operator who has made the reference, of the notice so far as referred.

(8) The Commissioner must consider whether the notice so far as referred is proportionate.

(9) The Board and the Commissioner must—

(a) give the operator concerned and the Secretary of State the opportunity to provide evidence, or make representations, to them before reaching their conclusions, and

(b) report their conclusions to—

(i) the operator, and

(ii) the Secretary of State.

(10) The Secretary of State may, after considering the conclusions of the Board and the Commissioner—

(a) vary or revoke the retention notice under section 94, or

(b) give a notice under this section to the operator concerned confirming its effect.

(11) But the Secretary of State may vary the notice, or give a notice under subsection (10)(b) confirming its effect, only if the Secretary of State's decision to do so has been approved by the Investigatory Powers Commissioner.

(12) A report or notice under this section is given to an operator by giving or publishing it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator.

(13) The Secretary of State must keep a retention notice under review (whether or not referred under subsection (1)).

…

95 Enforcement of notices and certain other requirements and restrictions

(1) It is the duty of a telecommunications operator on whom a requirement or restriction is imposed by—

(a) a retention notice, or

(b) section 92 or 93,

to comply with the requirement or restriction.

(2) A telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, must not disclose the existence or contents of a retention notice to any other person.

(3) The Information Commissioner, or any member of staff of the Information Commissioner, must not disclose the existence or contents of a retention notice to any other person.

(4) Subsections (2) and (3) do not apply to a disclosure made with the permission of the Secretary of State.

(5) The duty under subsection (1) or (2) **or under section 90(4A)** is enforceable (whether or not the person is in the United Kingdom) 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.

255 Further provision about notices under section 252 or 253

….

(10) The duty imposed by ~~**subsection (9)**~~ **subsection (8) or (9), or by section 257(3A),** is enforceable—

(a) in relation to a person in the United Kingdom, and

(b) so far as relating to a technical capability notice within subsection (11), in relation to a person outside the United Kingdom,

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.

….

257 Review of notices by the Secretary of State

…

~~**(3) There is no requirement for a person who has referred a notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (4).**~~

(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.

…

253 Technical capability notices

(1) The Secretary of State may give a relevant operator a technical capability notice under this section if—

(a) the Secretary of State considers that the notice is necessary for securing that the operator **or another relevant operator** has the capability to provide any assistance which ~~**the operator**~~ **such 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 proportionate to what is sought to be achieved by that conduct, and

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

(2) A "technical capability notice" is a notice—

(a) imposing on the relevant operator **(to whom the notice is given)** any applicable obligations specified in the notice, and

(b) requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations.

...

Clause 18

…

(10) "Telecommunications operator" means a person who—

(a) offers or provides a telecommunications service to persons in the United Kingdom, ~~**or**~~

(b) controls or provides a telecommunication system which is (wholly or partly)—

(i) in the United Kingdom, or

(ii) controlled from the United Kingdom**, 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.

…

Clause 19

87 Powers to require retention of certain data

…

(6) A retention notice comes into force—

(a) when the notice is given to the operator (or description of operators) concerned, or

(b) (if later) at the time or times specified in the notice.

(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.

(7) A retention notice is given to an operator (or description of operators) by giving, or publishing, it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates.

…

*Variation **~~or revocation~~** **, revocation or renewal** of notices*

94 Variation or revocation of notices

(1) The Secretary of State may vary a retention notice.

….

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.

255 Further provision about notices under section 252 or 253

…

(5) A relevant notice must be in writing.

(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.

…

Clause 20

267 Regulations

…

(3) A statutory instrument containing regulations under—

(a) section 12(4) or 271(2) which amend or repeal any provision of primary legislation,

(b) section 46(2),

(c) section 52(5),

(d) section 83,

(e) section 90(1),

(f) section 239,

(g) section 240(3),

(h) section 245,

(i) section 253,

(j) section 257(1), ~~**or**~~

(ja) section 258A(2), or

(k) paragraph 33 of Schedule 8,

may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

…

Clause 21

26 Members of Parliament etc.

(1) This section applies where—

(a) an application is made to the Secretary of State for the issue of a targeted interception warrant or a targeted examination warrant, and

(b) the purpose of the warrant is—

(i) in the case of a targeted interception warrant, to authorise or require the interception of communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) in the case of a targeted examination warrant, to authorise the selection for examination of the content of such communications.

(2) The Secretary of State may not issue the warrant without the approval of **–**

(a) the Prime Minister**, 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.

(2A) Condition A is that the Prime Minister is unavailable to decide whether to give approval under subsection (2).

(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 an individual under this section only if the individual holds the office of Secretary of State.

(2D) 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.

(2E) 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.

(3) In this section "member of a relevant legislature" means—

(a) a member of either House of Parliament;

(b) a member of the Scottish Parliament;

(c) a member of the National Assembly for Wales;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected for the United Kingdom.

Clause 22

111 Members of Parliament etc.

(1) Subsection (3) applies where—

(a) an application is made to the Secretary of State for a targeted equipment interference warrant, and

(b) the purpose of the warrant is to obtain—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(2) Subsection (3) also applies where—

(a) an application is made to the Secretary of State for a targeted examination warrant, and

(b) the purpose of the warrant is to authorise the selection for examination of protected material which consists of—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(3) The Secretary of State may not issue the warrant without the approval of the**—**

(a) Prime Minister**, 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) Subsection (5) applies where—

(a) an application is made under section 106 to a law enforcement chief for a targeted equipment interference warrant, and

(b) the purpose of the warrant is to obtain—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(5) The law enforcement chief may not issue the warrant without the approval of the Secretary of State unless the law enforcement chief believes that the warrant (if issued) would authorise interference only with equipment which would be in Scotland at the time of the issue of the warrant or which the law enforcement chief believes would be in Scotland at that time.

(6) The Secretary of State may give approval for the purposes of subsection (5) only with the approval of **–**

(a) the Prime Minister**, 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.

(7) In a case where the decision whether to issue a targeted equipment interference warrant is to be taken by an appropriate delegate in relation to a law enforcement chief under section 106(4), the reference in subsection (5) to the law enforcement chief is to be read as a reference to the appropriate delegate.

(7A) Condition A is that the Prime Minister is unavailable to decide whether to give approval under subsection (3) or (as the case may be) (6).

(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 an individual under this section only if the individual holds the office of Secretary of State.

(7D) 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.

(8) In this section "member of a relevant legislature" means—

(a) a member of either House of Parliament;

(b) a member of the Scottish Parliament;

(c) a member of the National Assembly for Wales;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected for the United Kingdom.

Clause 23

107 Restriction on issue of warrants to certain law enforcement officer

…

(3) The Director General **or a Deputy Director General** of the National Crime Agency may not issue a targeted equipment interference warrant on the application of a member of a collaborative police force unless the Director General **or the Deputy Director General (as the case may be)** considers that there is a British Islands connection.

"Collaborative police force" has the meaning given by paragraph 2 of Part 3 of Schedule 6.

…

Clause 24

121 Notification of modifications

(1) As soon as is reasonably practicable after a person makes a modification of a warrant under section 118, a Judicial Commissioner must be notified of the modification and the reasons for making it.

(2) But subsection (1) does not apply where—

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

(b) the modification is made by virtue of section 119(2), or (c) any of sections 111 to 114 applies in relation to the making of the modification.

(3) Where a modification is made by a senior official in accordance with section 119(1) or section 120(5)(a)(ii), the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

(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).

Clause 25

102 Power to issue warrants to intelligence services: the Secretary of State

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),

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

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, 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.

(2) But the Secretary of State may not issue a targeted equipment interference warrant under subsection (1) 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 authorise interference only with equipment which would be in Scotland at the time of the issue of the warrant or which the Secretary of State believes would be in Scotland at that time.

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

(3) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),

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

(c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of protected material for examination in breach of the prohibition in section 193(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), 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.

~~**(4) But the Secretary of State may not issue a targeted examination warrant under subsection (3) if 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.**~~

(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.

(5) A warrant is necessary on grounds falling within this subsection if it is necessary—

> (a) in the interests of national security,
>
> (b) for the purpose of preventing or detecting serious crime, or
>
> (c) 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.

(6) A warrant may be considered necessary on the ground falling within subsection (5)(c) only if the interference with equipment which would be authorised by the warrant is considered necessary for the purpose of obtaining information relating to the acts or intentions of persons outside the British Islands.

(7) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (5).

(8) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

(9) […]