Neutral Citation Number: [2023] EWCA Civ 926

Case No: CA-2022-001019, CA-2022-001635
& CA-2022-001594

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OFJUSTICE,
KING'S BENCH DIVISION,
DIVISIONAL COURT
THE RIGHT HONOURABLE LORD JUSTICE SINGH AND
THE HONOURABLE MR JUSTICE HOLGATE
[2018] EWHC 975 (Admin); [2019] EWHC 2057 (Admin) and
[2022] EWHC 1630 (Admin)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 04.08.2023

Before :

DAME VICTORIA SHARP, PRESIDENT OF THE KING'S BENCH DIVISION
LORD JUSTICE STUART-SMITH
and
LORD JUSTICE LEWIS
and

- -

Between :

THE KING **on the application of** **NATIONAL COUNCIL FOR CIVIL LIBERTIES**	**Appellant**
- and -	
(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT **(2) SECRETARY OF STATE FOR FOREIGN, COMMONWEALTH AND DEVELOPMENT AFFAIRS**	**Respondents**
-and-	
NATIONAL UNION OF JOURNALISTS	**Intervener**

- -
- -

Ben Jaffey KC, David Heaton and Sophie Bird (instructed by **Bhatt Murphy**) for the **Appellant**

Sir James Eadie KC, Gerry Facenna KC, Julian Milford KC, Michael Armitage, John Bethell and Cliodhna Kelleher (instructed by **Government Legal Department**) for the **Respondents**
Jude Bunting KC (instructed by **Bindmans**) for the **Intervener**

Hearing dates : 10-12 May 2023
- -

Approved Judgment

This judgment was handed down remotely at 2.30PM on 04 August 2023 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

THE PRESIDENT HANDED DOWN THE FOLLOWING JUDGMENT OF THE COURT:

Introduction

1. In this appeal the National Council for Civil Liberties, the appellant, challenges the compatibility of certain Parts of the Investigatory Powers Act 2016 ("the Act") with Articles 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention"). The appellant also challenges the compatibility of certain provisions of the Act with provisions of retained European Union ("EU") law.

2. The Act is concerned with the interception of communications, equipment interference in order to obtain communications or other information, the acquisition and retention of communications data, and the retention and examination of bulk personal datasets. It was introduced with the broad aim of consolidating investigatory powers previously contained in other statutes – and in certain respects, expanding and adding safeguards to various of those powers. Various of the provisions of the Act were brought into force between November 2016 and February 2019. Some powers concern the obtaining and examination of the content of communications. Other powers relate to "communications data", that is, data concerning matters such as where, when and by and to whom communications were sent but not the content of the communication.

3. The case itself and this appeal concerns in particular what are called "bulk powers", that is, powers which are not directed at particular individuals. This appeal also concerns equipment interference warrants granted under Part 5 of the Act which can be directed not only to particular individuals but also at groups, organisations or those engaged in particular activities.

4. Whether the arrangements governing access to data involve a justified interference with the right to respect for private and family life guaranteed by Article 8 and the right to freedom of expression in Article 10 is at the heart of this appeal. Those articles provide:

> "Article 8 Right to Respect for Private and Family Life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

and

> "Article 10 Freedom of Expression
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

The proceedings

5. By a claim form issued on 28 February 2017, the appellant, a well-known civil liberties organisation, brought a wide-ranging claim for judicial review. The claim challenged Parts 3, 4, 5, 6 and 7 of the Act on the ground that certain provisions violated Articles 8 and 10 of the Convention and also violated EU law. At that stage, the United Kingdom was a Member State of the EU and bound by EU law.

6. The Act is a lengthy and complicated piece of legislation. The Divisional Court recognised that a proper understanding of this case would be assisted by a summary of the Act's provisions, and attached to its judgment an Annex ("the Annex") prepared by the parties, which contained an agreed overview of the Act, subject to three "riders" from the appellant, then claimant, which were identified where relevant. For convenience we attach the Annex to this judgment. A recitation of the substance of the provisions under challenge is nonetheless unavoidable.

7. By way of introduction however it is sufficient to say that Parts 3 and 4 of the Act concern authorisations and notices for the retention and authorisation of communications data; Part 5, concerns warrants for targeted equipment interference for the obtaining of communications and equipment data and other information; Part 6, Chapter 1, concerns bulk interception warrants; Part 6, Chapter 2, concerns bulk acquisition warrants; Part 6, Chapter 3, concerns bulk

equipment interference warrants; and Part 7, concerns warrants for the retention and examination of bulk personal datasets.

8. The Divisional Court (Singh LJ and Holgate J) dealt with the claim over the course of three very substantial judgments. The first judgment dealt with the compatibility of the provisions of Part 4 of the Act with certain aspects of EU law: see [2018] EWHC 975 (Admin) ("the first EU law Judgment"). The second judgment dealt with the challenge pursuant to the Human Rights Act 1998 ("the HRA") and the Convention: see [2019] EWHC 2057 (Admin) [2020] 1 WLR 243 ("the Convention Judgment"). This was the only part of the proceedings below in which the Intervener, the National Union of Journalists, took part; and it is to the Convention Judgment that the Annex was attached. The third judgment dealt with the compatibility of provisions of Parts 3, 4, 5, 6 and 7 of the Act with EU law: see [2022] EWHC 1630 (Admin) ("the second EU law Judgment").

9. The fact that this litigation has extended over a six-year period has added various layers of complexity to the case and to this appeal. In the result, we do not have the benefit of a reasoned judgment at first instance on some of the issues which are central to this appeal, the evidence is not necessarily apt to meet those issues; and the case as argued before us is different in certain material respects to the claim as originally mounted and argued before the Divisional Court. We should briefly explain how this state of affairs has come about.

    i) The first EU law Judgment concerned only the challenge under EU law to Part 4 of the Act, as this was the only relevant Part in force at the time. The judgment itself focussed almost entirely on remedies. Materially identical provisions in the Data Retention and Investigatory Powers Act 2014 ("DRIPA") had already been declared incompatible with EU law in two respects by the Court of the European Union ("CJEU") on a reference from this court: see *R (Watson and others) v Secretary of State for the Home Department (Open Rights Group and others intervening)* [2017] Q.B. 771. In the light of concessions made by the respondents, the Divisional Court made a declaration permitting the respondents six months to amend the Act. Amendments were made by way of secondary legislation (The Data Retention and Acquisition Regulations 2018 ("the 2018 Regulations")) and renewed Codes of Practice, which came into effect in mid-2018. The Divisional Court either dismissed further points of challenge or these were stayed, pending the outcome of a reference to the CJEU made by the Investigatory Powers Tribunal ("the IPT") in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2018] 2 All ER 166.

    ii) The Convention Judgment dealt with the entirety of the challenge under the Convention. The hearing of this part of the claim took place in June 2019.

    iii) By the time of that hearing, the First Section of the European Court of Human Rights ("the European Court") had handed down its judgment in *Big Brother Watch v United Kingdom* (App. Nos. 58170/13, 62322/14

and 24960/15) and its decision had been referred to the Grand Chamber. The Grand Chamber's decision was subsequently handed down in May 2021 and found broader violations of Articles 8 and 10 in respect of section 8(4) of a predecessor statute, the Regulation of Investigatory Powers Act 2000 ("RIPA"): see *Big Brother Watch v United Kingdom* (2022) 74 EHRR 17 ("*Big Brother Watch*"). We deal with this case in more detail at paragraphs 13 to 35 below. In broad terms however, the applicants in that case challenged amongst other things, the compatibility of the regimes governing bulk interception in RIPA.

iv) In view of the decision of the First Section, the appellant did not pursue parts of the Convention challenge pending the decision of the Grand Chamber. The Divisional Court decided not to delay giving the Convention Judgment, pending the Grand Chamber's decision and dismissed what was left of the Convention challenge.

v) *Big Brother Watch* is now heavily relied on by the appellant for significant parts of this appeal; indeed, it is central to the appellant's challenge on its first three grounds, which have occupied a substantial part of the argument before this Court. Further, the respondents accept that certain provisions of Chapter 1 of Part 6 need to be amended in the light of the judgment in *Big Brother Watch* and is proposing to make a remedial order under section 10 of the HRA. This order will substitute a new section 154 of the Act and will provide additional safeguards for confidential journalistic material. Although not yet in force, we have proceeded on the basis that that remedial order has been made and we have considered the safeguards as they will be under the Act once amended.

vi) The second EU law Judgment dealt with the outstanding elements of the EU law challenge namely (i) those stayed behind the CJEU's judgment in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* Case (C-623/17) [2021] 1 WLR 4421, which was handed down in October 2020 alongside a related judgment in three joined cases: *La Quadrature du Net v Premier Ministre* (Joined Cases C-511/18, C-512/18 and C-520/18) [2021] 1 WLR 4457 ("*La Quadrature*"); and (ii) the challenge to those parts of the impugned provisions of the Act not in force in 2018, namely Parts 3 and 5 to 7 of the Act. The second EU Judgment also dealt with the effect of the 2018 Regulations as the appellant contended the amendments made to the relevant legislation following the first EU Judgment were inadequate. The Divisional Court upheld the appellant's challenge in one narrow respect, but otherwise dismissed this part of the challenge.

vii) On 22 July 2022, the Divisional Court granted permission to appeal on three EU law grounds arising from the first EU law Judgment and the Second EU law Judgment. The Divisional Court also separately (on 28 April 2022, after *Big Brother Watch* had been handed down) granted permission to appeal on five grounds arising from the Convention Judgment.

Grounds of Appeal and our decision

10. There are eight grounds of appeal. Grounds 1 to 5 concern the Convention Judgment. Those grounds identify five areas where it is said that the Divisional Court erred in failing to find that provisions of the Act were incompatible with Article 8 and (in the case of the first three grounds) Article 10 of the Convention: see appellant's notice dated 20 May 2022. Grounds 6 to 8 (our numbering) concern three EU law related grounds raised in respect of the first and second EU Judgments: see appellant's notice dated 12 August 2022.

11. The Grounds may be summarised as follows:

    i) The Act does not provide sufficient safeguards for the protection of journalistic material. Part 6 Chapter 1 (as it is to be amended: see paragraph 9 above) (a) does not provide for the application of safeguards where search terms are to be used which are known to be connected to a journalist or news organisation or which would make the selection of confidential journalistic material likely and (b) has no provision that there must be an overriding requirement in the public interest for the examination of such material. Further, there are no adequate safeguards relating to the selection of confidential journalistic material in Parts 3, 4, 5, 6 (Chapters 2 and 3) and 7 in relation to those matters. Further, it is contended that various provisions of the definition of journalistic material reduce the scope of protection in a way that is incompatible with Articles 8 and 10 of the Convention.

    ii) Parts 5, 6 and 7 of the Act do not provide adequate safeguards against the risk of abuse. In particular, there is no requirement for the categories or types of selectors (i.e., search terms) to be identified in the application for a warrant. There is no requirement of prior internal authorisation of "strong selectors", that is search terms linked to identifiable individuals. The provisions are inadequate in failing to exclude material related to a person in the British Islands in relation to secondary data and non-protected material in Part 6 Chapters 1 and 3, failing to apply that safeguard in relation to communications data in Part 6 Chapter 2, and failing to apply such a safeguard to Part 7;

    iii) Parts 5, 6 and 7 of the Act do not have adequate safeguards in relation to sharing of material with overseas authorities;

    iv) Part 7 contains an impermissibly broad set of provisions providing for retention of bulk personal datasets and so is not in accordance with law for the purposes of Article 8 of the Convention and also contains inadequate safeguards relating, amongst other things, to the deletion, disclosure and copying of such datasets;

    v) Parts 3, 4, 5, 6 and 7 contain inadequate safeguards for the protection of lawyer-client communications;

vi) Parts 3, 4, 5, 6 and 7 provide for general and indiscriminate retention and access to data and so retained EU law requires them to have certain safeguards;

vii) Parts 3, 4, 5 and 7 (and in certain circumstances Part 6) of the Act provide for access to data for a purpose other than national security without there being prior independent authorisation;

viii) Insofar as the provisions of the Act do not comply with the requirements of Articles 8 and 10 of the Convention following the decision of the Grand Chamber in *Big Brother Watch*, those provisions do not comply with Articles 7 and 11 of the Charter of Fundamental Rights of the European Union ("the Charter") and equivalent general principles of EU law.

12. In brief summary, our conclusions are first, that the provisions challenged in this appeal are, with one exception, Convention compliant, and secondly, that those provisions do not violate EU law. More specifically:

i) The amended provisions governing bulk interception warrants under Chapter 1 of Part 6 are sufficient to ensure adequate safeguards for the protection of confidential journalistic material;

ii) The provisions in Parts 3, 4, 5, Chapter 2 of Part 6 and Part 7 provide sufficient safeguards in this respect;

iii) Whether the provisions of Chapter 3 of Part 6 are sufficient to provide adequate safeguards for the protection of a journalist's sources or confidential journalistic information in relation to communications obtained by means of a bulk equipment interference warrant will be remitted to the Divisional Court for consideration;

iv) The safeguards provided in Parts 5, 6 and 7 do provide adequate safeguards in connection with the use of criteria for examination of material; Parts 5, 6 and 7 do provide adequate safeguards governing the sharing of data transferred to authorities in other states save that those safeguards are not in accordance with law so far as material from bulk personal data sets are concerned as they are not contained in any legislation, code, or publicly available policy or other document;

v) Part 7 is not impermissibly wide and does provide sufficiently detailed rules governing retention and use of material; Parts 3, 4, 5, 6 and 7 do provide adequate safeguards for the protection of legally privileged material; Parts 3, 4, 5, 6 and 7 do not provide for the general and indiscriminate retention of data within the meaning of retained EU law and do provide adequately for prior independent authorisation of access to data. On the facts of this case, no question of the need for any remedy for any alleged violation of any article of the Charter arises.

Big Brother Watch v United Kingdom

13. In *Big Brother Watch*, the Grand Chamber considered the compatibility of the provisions of section 8(4) of RIPA with Articles 8 and 10 of the Convention. Section 8(4) was repealed on 27 December 2018. Section 8(4) is materially different to the legislative provisions under consideration in this appeal and the new legislation includes additional safeguards.

14. Section 8(4) of RIPA conferred a power on the Secretary of State to issue a warrant for "the interception of external communications in the course of their transmission by means of a telecommunication system". The Secretary of State was also required to issue a certificate setting out a description of the intercepted material which the Secretary of State considered it necessary to examine and stating that he or she considered that it was necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as relevant to national security.

15. The complaint in *Big Brother Watch* concerned "the bulk interception of cross-border communications by the intelligence services" (paragraph 322). The Grand Chamber viewed bulk interception as a gradual process where the degree of interference with Article 8 rights increased as the process progressed. It acknowledged that bulk interception regimes did not all follow the same model, and that the different stages of the process would not necessarily be discrete or followed in strict chronological order. Subject to those caveats, the Grand Chamber considered that the bulk interception process could be described in four stages: (i) the interception and initial retention of communications and related communications data; (ii) the application of specific selectors to the retained communications or communications data; (iii) the examination of selected communications and communications data by analysts; and (iv) the retention and use of the product of the analysis, including sharing with third parties (paragraph 325). These stages are then described.

16. The Grand Chamber considered that Article 8 applied to each of those four stages; that the initial interception followed by the discarding of parts of the communications did not constitute a particularly significant interference; and that the degree of interference increased as the bulk interception process progressed (paragraph 330).

17. The Grand Chamber noted that any interference with a person's Article 8 rights could only be justified if it is in accordance with law, pursues one or more legitimate aims and is necessary in a democratic society to achieve such aims. The requirement that the interference be "in accordance with law" required the impugned measure to have a basis in domestic law, to be accessible, and to be foreseeable (that is, that there must be sufficiently clear rules to give citizens an adequate indication as to the circumstances in which, and the conditions on which, public bodies may resort to such measures). Furthermore, the lawfulness of the interference was closely related to whether the interference was "necessary", in particular by providing adequate and effective safeguards against abuse (paragraphs 332 to 334).

18. The Grand Chamber accepted that bulk interception regimes fell within the range of a state's discretion. The decision to operate a bulk interception regime in order to identify threats to national security or to essential national interests fell within this margin of appreciation (paragraph 340). It then explained how bulk interception was generally directed at international communications, and was not necessarily targeted at specific individuals but could be used for that purpose. At that stage, individuals could be targeted by the use of what it termed "strong selectors", i.e., search terms for examining the material which are related to individuals (paragraphs 344 to 348).

19. Against that background, the Grand Chamber set out the approach to be followed in bulk interception cases. The grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted must be identified (paragraph 348). Bulk interception should be authorised by an independent body who should be informed both of the purpose of the interception and the bearers (that is the communication systems) subject to interception. Dealing with the examination of intercepted material, the authorisation should identify the "types or categories of selectors to be used" (paragraph 354). Further, the use of "strong selectors", that is, search terms linked to identifiable individuals, must be justified by the intelligence services by reference to necessity and proportionality and be recorded and subject to a process of prior internal authorisation (paragraph 355). There should be supervision of the bulk interception process by an independent authority and an effective remedy should be available to anyone who suspected that his or her communications had been intercepted (paragraphs 356 and 357).

20. The Grand Chamber summarised its approach in the following way at paragraph 360:

> "In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to "end-to-end safeguards" (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse…".

21. Further, at paragraph 361, it said this:

> "In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six Weber safeguards. More specifically, in addressing jointly "in accordance with the law" and

> "necessity" as is the established approach in this area (see Roman Zakharov, cited above, § 236 and Kennedy, cited above, § 155), the Court will examine whether the domestic legal framework clearly defined:
>
> the grounds on which bulk interception may be authorised;
>
> the circumstances in which an individual's communications may be intercepted;
>
> the procedure to be followed for granting authorisation;
>
> the procedures to be followed for selecting, examining and using intercept material;
>
> the precautions to be taken when communicating the material to other parties;
>
> the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
>
> the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
>
> the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."

22. The Grand Chamber offered guidance on the safeguards necessary in connection with the communication of intercepted material to foreign states or international organisations. The circumstances in which such a transfer may take place should be set out clearly in domestic law. The transferring state should make sure that the receiving state has adequate safeguards in place, particularly as regards secure storage and the restriction of onwards transmission. Heightened safeguards would be necessary where the material required special confidentiality such as confidential journalistic material. Transfer should be subject to independent control (paragraph 362).

23. It did not consider that the acquisition of communications data through bulk interception was necessarily less intrusive than the acquisition of content. It therefore considered that the interception, retention and searching of communications data should be analysed by reference to the same safeguards as those applicable to content. However, in view of the different character of communications data, and the different way in which they were used by the intelligence services, the legal provisions governing the treatment of communications data did not have to be identical in every respect to those governing the treatment of content (paragraphs 363 to 364).

24. The Grand Chamber then carried out an assessment of the whole process governing the bulk interception of communications and related communications data to determine whether viewed as a whole it contained "sufficient end-to-end safeguards" to provide adequate and effective safeguards against arbitrariness and the risk of abuse. In that regard, it considered the eight features that it had identified.

25. First, the grounds upon which bulk interception could be authorised under RIPA were that the Secretary of State was satisfied that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or safeguarding the economic well-being of the United Kingdom. Although broad, the identification of those as grounds for bulk interception was not of itself considered deficient (paragraphs 368 to 371).

26. Secondly, the circumstances in which an individual's communications might be intercepted under section 8(4) of RIPA were sufficiently foreseeable. The warrant authorised the interception of those bearers (or communication systems) most likely to be carrying external communications of interest to the intelligence service (paragraphs 372 to 376).

27. Thirdly, the Secretary of State alone had the power to issue a warrant. There was no requirement for authorisation by a body independent of the executive. Consequently, "the section 8(4) regime lacked one of the fundamental safeguards: namely that bulk interception should be subject to independent authorisation at the outset" (paragraph 377). (The position is different under the Act, where there is the "double-lock", that is, the decision to grant a warrant is taken by the Secretary of State but has to be approved by a Judicial Commissioner.)

28. In terms of the level of scrutiny provided for, the procedure for granting authorisation involved the following. The application had to include a description of the communications to be intercepted, details of the communications service providers, an assessment of the feasibility of the operation, a description of the conduct to be authorised, an explanation of why interception was necessary for the permitted purposes for which authorisation had to be granted and various assurances. The Secretary of State would have to provide a certificate setting out the intercepted material that the Secretary of State considered it necessary to examine. The Grand Chamber considered that that would mean that the Secretary of State would be informed of the purposes of the operation (national security, prevention or detection of serious crime, or protection of the economic well-being of the United Kingdom) and would have to assess whether the warrant was necessary for those purposes and proportionate for what it sought to achieve.

29. Fourthly, the Grand Chamber noted that the application for a warrant did not have to include an indication of the categories of "selectors" or search terms to be employed and as a consequence there was no possibility for their necessity and proportionality to be assessed at the authorisation stage. Given that the choice of search terms determined which communications would be eligible for examination by an analyst, the Grand Chamber considered that the categories or types of "selectors" (or search terms) should be identified in the authorisation

and that "strong selectors" (or search terms) linked to identifiable individuals should be subject to prior internal authorisation. In those circumstances, it considered that "the absence of any oversight" of the categories of selectors at the authorisation stage was "a deficiency in the section 8(4) regime". The Grand Chamber also noted that there was no prior internal authorisation of "strong selectors" linked to identifiable individuals (although analysts had to record and justify the use of such selectors or search terms and that was subject to subsequent independent supervision (paragraphs 378 to 383)). Further, the certificate that the Secretary of State had to provide under section 8(4) of RIPA was couched in such general and insufficiently precise terms, that did not provide any meaningful restriction on the process of selecting material for examination (paragraphs 384 to 391). The Grand Chamber considered that subject to the "deficiencies relating to the authorisation of selectors" and the general nature of the section 8(4) RIPA certificate, the circumstances in which the intercepted material could be selected were sufficiently foreseeable for the purposes of Article 8 of the Convention (paragraph 391).

30. In relation to the remaining four criteria, the Grand Chamber considered that the safeguards in place were sufficiently clear and satisfactory to guarantee against abuse (paragraphs 392 to 399 in relation to communication to other states, paragraphs 400 to 405 on duration, storage and destruction of intercepted material, paragraphs 406 to 412 on supervision of the regime and paragraphs 413 to 415 on ex post facto review).

31. The Grand Chamber considered related communications data and identified the same three deficiencies, namely the absence of prior independent authorisation, the failure to identify the categories of selectors in the application, and the failure to subject selectors linked to identifiable individuals to prior internal authorisation, together with the general nature of the section 8(5) certificate. It did not consider that two other matters carried decisive weight in the assessment, namely that where communications data were examined by reference to a selector referable to an individual known to be in the British Islands that selector or search term did not need approval as necessary and proportionate by the Secretary of State, and that communications data could be kept for a longer period than communications (paragraphs 416 to 423).

32. In the light of that assessment, the Grand Chamber concluded that "bulk interception is of vital importance to Contracting States in identifying threats to their national security" (paragraph 424). At paragraph 425 to 427, it said this:

> "425. Nonetheless, the Court recalls that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for private life (see paragraph 347 above). Therefore, in a State governed by the rule of law, which is expressly mentioned in the Preamble to the Convention and is inherent in the object and purpose of Article 8 (see Roman Zakharov, cited above, § 228), the Court considers that, when viewed as a whole, the section 8(4) regime, despite its safeguards, including some robust ones as highlighted above (see, for example, paragraphs

> 412 and 415 above), did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it has identified the following fundamental deficiencies in the regime: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation (see paragraphs 377-382 above). These weaknesses concerned not only the interception of the contents of communications but also the interception of related communications data (see paragraph 416 above). While the IC Commissioner provided independent and effective oversight of the regime, and the IPT offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, these important safeguards were not sufficient to counterbalance the shortcomings highlighted at paragraphs 377-382 above.
>
> 426. In view of the aforementioned shortcomings, the Court finds that section 8(4) did not meet the "quality of law" requirement and was therefore incapable of keeping the "interference" to what was "necessary in a democratic society."
>
> 427. There has accordingly been a violation of Article 8 of the Convention."

33. The Grand Chamber then considered whether there had been a violation of Article 10 of the Convention. It recognised that freedom of expression constituted one of the essential foundations of a democratic society. It noted that the safeguards for the press were particularly important and that the protection of journalistic sources was one of the cornerstones of a free press. It noted that orders to divulge a source could have a detrimental impact, but considered that the search of a journalist's home or workplace to reveal or confirm the identity of the journalist's sources constituted a more drastic measure (paragraphs 442 to 445).

34. It set out its general approach to Article 10 in the context of bulk interception. It noted that under the section 8(4) RIPA regime, the intelligence services could access confidential journalistic material either intentionally, through the use of search terms connected to a journalist or news organisation, or unintentionally as a consequence of the bulk interception operation accessing material which turned out to be confidential journalistic information. It considered that, before the intelligence services used selectors which were known to be connected to a journalist, or which would make the selection of confidential journalistic material highly probable, those search terms should have been authorised by an independent body who could determine whether these were justified by an

overriding requirement in the public interest (paragraphs 445 to 449). Domestic law should also contain safeguards regarding storage, examination, use, onward transmission and destruction (paragraph 450). Applying that approach to the regime in issue there, the Grand Chamber identified two weaknesses. These were first that where the intention was to access confidential journalistic material, or where the use of particular search terms made that highly probable, there was no provision for authorisation by an independent person who could determine whether that was justified by an overriding public interest requirement. Secondly, there were insufficient safeguards for storing or examining such material once it became apparent that such material had been examined. In view of those weaknesses, the European Court found a breach of Article 10 (paragraphs 451 to 451).

35. The Grand Chamber also considered the application of Article 10 to the regime in RIPA governing the bulk acquisition of communications data. It noted that the relevant code of practice required that where an application was intended to determine the source of journalistic information there had to be an overriding requirement in the public interest for such a warrant. However, those provisions of the code of practice only applied where the purpose was to determine a source and did not apply in every case where a request was made for the communications data of a journalist or where such an intrusion was likely. Further, there was no requirement restricting access to serious crime (as opposed to crime). For those reasons, the Grand Chamber found that there had been a violation of Article 10 in relation to the regime governing the acquisition of communications data as the regime was not in accordance with law (paragraph 517).

The Background to the Act

36. Before addressing the legislative scheme in detail as we must, it is important to have in mind the problems to which the Act is addressed and the degree of scrutiny given to the provisions of the Act prior to its enactment. These matters are fully set out in the Convention Judgment (handed down, as we have said, before the Grand Chamber's decision in *Big Brother Watch*) in the following terms:

> "18. The threats to security which the United Kingdom and members of the public face are well known and hardly need evidence, although there is plenty of such evidence which has been placed before this court: see in particular the first witness statement of James Dix, acting Head of the Investigatory Powers Unit in the Office for Security and Counter-terrorism at the Home Office. By way of example, in 2017 there were five terrorist attacks, in London and Manchester, which resulted in 36 deaths. The organisations Daesh (sometimes called "Islamic State" or "ISIL") and Al Qa'ida continue to pose threats to British nationals and others around the world. There is an increasing threat from far-right extremism. Further, this country faces "sustained hostile activity from certain states": see a speech given by the Director General of

MI5 (Sir Andrew Parker) in Berlin on 14 May 2018, quoted at para 15 of Mr Dix's first witness statement.

19. In addition, there is an acknowledged need to support the investigation and punishment of serious organised crime, including offences against children. It is also well known that those who would wish to do harm to this country and its inhabitants are increasingly able to make use of encryption and the "dark web", which Mr Dix describes, at para 20 of his first witness statement, as "a space in which information can be exchanged anonymously beyond the reach of law enforcement".

20. Against that background, Mr Dix expresses the following opinion to this court at para 24 of his first witness statement: "The investigatory powers under challenge in this claim make a very significant contribution to tackling the kind of threats set out above: indeed, they are essential for doing so." At para 28 he tells this court that the use of bulk data is among the few effective methods to counter the illicit use of the dark web. Further, as he points out at para 29, in certain parts of the world the United Kingdom has no physical presence, so there are often no initial intelligence leads on emerging threats, whether from terrorists, serious criminals or state-based threats: "Bulk powers allow security and intelligence agencies to identify and map out known and evolving networks, in turn enabling further intelligence gathering on likely threats."

21. Finally, in this context, it is important to note that the situation can often be a "dynamic" one. At para 30 of his first witness statement Mr Dix states that:

"Bulk powers also allow the security and intelligence agencies to respond at pace, quickly identifying threats and ruling individuals in or out of investigations. Bulk powers are made more important by the fact that terrorist threats are increasingly diverse in nature and can escalate with increasing speed through the use of the internet to radicalise supporters and plan and execute attacks."

22. The utility of bulk powers is illustrated by the fact that, as Mr Dix says at para 32:

"Bulk data analysis has played a significant part in every major counter terrorism investigation over the last decade, including in each of the seven terrorist attack plots disrupted between 2014 and the publication of the Operational Case in 2016."

(That is a reference to the Government's operational case for bulk powers, which was published during the passage of the Investigatory Powers Bill.)

23. Mr Dix states at para 33 of his first witness statement that, before the 2016 Act, many similar powers, including bulk powers, could be found in a range of different statutes, in particular the following:

(1) Powers to intercept communications, including in bulk, were provided for in Part 1, Chapter I of RIPA .

(2) Equipment interference was provided for in powers contained in the Intelligence Services Act 1994 and the Police Act 1997 .

(3) Bulk personal datasets could be acquired using information gathering powers in the Intelligence Services Act 1994 ("ISA") and the Security Services Act 1989 ; and processes for their retention and examination were set out in published agency handling arrangements.

(4) Retention of communications data was provided for in the Data Retention and Investigatory Powers Act 2014 (as amended by the Counter-terrorism and Security Act 2015) and the Anti-terrorism, Crime and Security Act 2001 .

(5) The targeted acquisition of communications data was primarily provided for in Part 1, Chapter II, of RIPA .

(6) Bulk acquisition of communications data was provided for in the Telecommunications Act 1984 .

24. Prior to the Investigatory Powers Bill, Mr Dix states (at para 34) that there were three reviews of investigatory powers undertaken. The first was *A Question of Trust* (June 2015 by David Anderson QC, who was at that time the Independent Assessor of Terrorism Legislation and is now Lord Anderson of Ipswich QC). In March 2015 there was the *Report on Privacy and Security* by the Intelligence and Security Committee of Parliament ("ISC"). In July 2015 there was a report by a panel convened by the Royal United Services Institute ("RUSI"). Mr Dix states that all three reviews agreed that the use of the existing complement of investigatory powers remained vital to the UK's national security and other interests. They made 198 recommendations as to the way in which these powers should be overseen. He says, at para 36, that the central recommendation by Lord Anderson in *A Question of Trust* was that:

"A comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive powers that it may be necessary for the public authorities to use." (Executive summary, para 10.)

25. During the passage of the 2016 Act through Parliament there was pre-legislative scrutiny by three committees: the House of Commons Science and Technology Committee, which produced a report entitled "Investigatory Powers Bill: Technology Issues" in January 2016; the ISC, which produced a report on the Bill in 2016; and a report by the Joint Committee on the Bill produced in February 2016. The Joint Committee alone took 2,364 pages of written evidence and transcripts of oral evidence from stakeholders across society. The Joint Committee recommended that the Government should publish a fuller justification for each of the bulk powers alongside the Bill (recommendations 23 and 28). This was done in the Operational Case for Bulk Powers. The Government also published an amended operational case for the retention of internet connection records following a recommendation from the Joint Committee.

26. The Investigatory Powers Bill was introduced in Parliament on 1 March 2016, having been previously published in draft form for pre-legislative scrutiny. The Government published its own formal response to that scrutiny.

27. Furthermore, at the same time as the Bill was introduced, draft codes of practice were published so that Parliament would have the opportunity to consider those alongside the Bill.

28. The Government also commissioned the Independent Reviewer of Terrorism Legislation to conduct a detailed review of the operational case for bulk powers, which was published by Lord Anderson as the "Report of the Bulk Powers Review" in August 2016.

29. The Government itself also published an operational case for use of communications data by public authorities.

30. The new regime introduced by the 2016 Act is now largely operational, with the majority of the powers under the Act having been brought into force during the course of 2018. The provisions relating to equipment

interference and interception were commenced for the intelligence services on 27 June 2018, with interception for law enforcement commenced on 26 September 2018 and equipment interference on 5 December 2018. A commencement order in respect of the bulk communications data and bulk personal dataset provisions was made on 18 July 2018, and the provisions concerning the issuing of warrants came into force on 22 August 2018. The final part of the Act to be commenced was Part 3, which was commenced on 5 February 2019.

31. In the meantime, earlier, in 2017, there had been established the office of the IPC. The 2016 Act requires the IPC to be a person who holds or has held high judicial office. The first and current IPC is Sir Adrian Fulford, who is a serving Lord Justice of Appeal.[1] He has a staff of some 50 people, including those with technical expertise. His office includes 15 judicial commissioners ("JCs"), who also have to be persons who hold or have held high judicial office: they include retired members of the High Court, the Court of Appeal and the Supreme Court. The IPC's deputy is Sir John Goldring, a retired member of the Court of Appeal.

32. In addition, in anticipation of the full implementation of Part 3 of the Act, which is expected to occur by the end of 2019, there has been created the Office for Communications Data Authorisations ("OCDA"), which is under the remit of the IPC.

33. In the view of many commentators the most significant and innovative provision in the 2016 Act is the creation of a "double lock" for warrants authorising use of certain intrusive powers. Where this applies the Act requires that an independent JC must approve the decision of the Secretary of State (or, where relevant, Scottish Minister/law enforcement chief). The UN Special Rapporteur on the Right to Privacy (Joseph Cannataci), following a visit to the UK, observed in his "end of mission statement" that this element of judicial review "assisted by a better-resourced team of experienced inspectors and technology experts is one of the most significant safeguards introduced by the IPA ": see his report of June 2018, p 2."

[1] The current IPC is Sir Brian Leveson, former President of the Queen's Bench Division and a former Lord Justice of Appeal. His deputy is Sir John Goldring, a former Lord Justice of Appeal.

The Legislative Structure

37. Any assessment of the compatibility of the provisions of the Act with the Convention or retained EU law, will, critically, involve consideration of the whole scheme of the Act and relevant Codes of Practice, and a close assessment as well as an overview, of the safeguards governing the regime.

The General Privacy Protections

38. Part 1 of the Act sets out an overview of the Act and general privacy duties. Section 1 provides so far as material that:

> "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,
>
> …..
>
> (vi) elsewhere in the law.
>
> (6) The regimes provided for by Parts 2 to 7 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 with bulk personal dataset warrants.
>
> (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."

39. Section 2 of the Act sets out general duties on public authorities in relation to privacy, dealing with the powers conferred by Parts 3, 4, 5, 6 and 7 of the Act. It provides, so far as material, that:

> "(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)."

The Scope of the Act

40. Part 2 of the Act deals with targeted interception warrants. These are warrants which authorise the interception of communications in relation to a particular person or organisation, or a single set of premises. Such a warrant may extend to groups who share a common purpose or carry on a common activity or more than one person or organisation or premises where the warrant is for the purposes of a single investigation or operation (sections 15 and 17 of the Act). No issue arises on this appeal in relation to these warrants.

41. As already mentioned, in Parts 3 and 4 the Act deals with the bulk retention and acquisition of communications data. In Part 5 it deals with targeted equipment interference warrants. Part 6 deals with bulk powers governing bulk interception, bulk acquisition and bulk equipment interference warrants which are dealt with in Chapters 1, 2 and 3 of Part 6, respectively. Part 7 deals with the retention and examination of bulk personal datasets.

42. It is convenient to start with the provisions in Part 6.

Part 6 Chapter 1 - Bulk Interception warrants

43. A bulk interception warrant is a warrant that authorises the interception of communications or the obtaining of secondary data, and the examination and disclosure of the content of the intercepted communications or secondary data. Further, the main purpose of the warrant must be the interception of "overseas-related communications" (or obtaining secondary data from such communications), that is, communications sent or received by individuals who are outside the British Islands (section 136 of the Act). The purpose therefore is to facilitate the interception of cross-border communications by the intelligence services.

44. An application for a warrant may only be made on behalf of the head of an intelligence service (they are not available to public authorities generally). The power to issue the warrant must be exercised by the Secretary of State personally. The Secretary of State may only grant a bulk interception warrant if he or she considers, amongst other things, that the warrant is necessary "in the interests of national security" or for national security reasons together with the prevention or detection of serious crime or in the interests of the economic well-being of the United Kingdom so far as relevant to national security. The Secretary of State must also consider whether the conduct authorised by the warrant is proportionate and if the examination of intercepted communications or secondary data is necessary for each of the specified operational purposes: sections 138 and 141 of the Act. The Secretary of State must also comply with the obligations imposed by section 2 of the Act, including considering whether what is sought could be reasonably achieved by less intrusive means, whether the level of protection for the information should be higher because of its particular sensitivity, and any other aspects of the public interest in the protection of privacy.

45. The issuing of a bulk interception warrant is subject to prior approval by a Judicial Commissioner, that is, a person who holds or has held high judicial

office (section 227(2)). Such persons will have experience of independent and impartial scrutiny of the exercise of executive powers. The need for the warrant to be granted personally by the Secretary of State and approved by the Judicial Commissioner is what is referred to as the "double-lock." That safeguard did not exist under RIPA where there was no provision for prior approval by an independent judicial body. Section 140 of the Act provides, so far as material, that:

> "140 Approval of warrants by Judicial Commissioners
>
> (1) In deciding whether to approve a decision to issue a warrant under section 138, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—
>
> (a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section,
>
> (b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
>
> (c) whether—
>
> (i) each of the specified operational purposes (see section 142) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, and
>
> (ii) the examination of intercepted content or secondary data for each such purpose is necessary as mentioned in section 138(1)(d)(ii), and
>
> (d) any matters taken into account in accordance with section 139.
>
> (2) In doing so, the Judicial Commissioner must—
>
> (a) apply the same principles as would be applied by a court on an application for judicial review, and
>
> (b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).
>
> ….."

46. The reference to operational purposes is a reference to one of the requirements that must be met by a warrant. Section 142 provides, so far as material, as follows:

"142 Requirements that must be met by warrants"

(1) A bulk interception warrant must contain a provision stating that it is a bulk interception warrant.

(2) A bulk interception warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk interception warrant must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination.

(4) The operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which intercepted content or secondary data obtained under bulk interception warrants may be selected for examination.

(5) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

(6) An operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State.

(7) The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 138(1)(b) or (2).

(8) At the end of each relevant three-month period the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament.

(9) In subsection (8) "relevant three-month period" means—

(a) the period of three months beginning with the day on which this section comes into force, and

(b) each successive period of three months.

(10) The Prime Minister must review the list of operational purposes at least once a year.

> (11) In this Chapter "the specified operational purposes", in relation to a bulk interception warrant, means the operational purposes specified in the warrant in accordance with this section."

47. Further provisions governing the information that must be included in an application for a bulk interception warrant are set out in the Interception Code of Practice ("the Interception Code") issued pursuant to Schedule 7 to the Act. That explains that the application should contain the background to the application, a description of the communications to be intercepted and the conduct to be authorised, the operational purposes for which the data may be selected for examination and an explanation of why examination is or may be necessary, and a description of why it is necessary to authorise the conduct for one of the statutory purposes for which warrants may be granted which must always include an explanation of why the interception is necessary in the interests of national security and other matters (paragraph 6.20 of the Interception Code). The Judicial Commissioner is also able to seek clarification or additional information in relation to a warrant application and there is an obligation on the agency requesting the warrant to provide information and documents if requested to do so (section 235 of the Act and paragraph 6.29 of the Code).

48. The Secretary of State must satisfy herself that arrangements are in force providing safeguards governing the use and retention of material (section 150). The arrangements must ensure that the number of people to whom material is disclosed, and the extent to which it is made available and copied is limited to the minimum necessary (section 150). The arrangements must also ensure that the selection of intercepted communications and secondary data is carried out only for the operational purposes specified in the warrant and if that is necessary and proportionate (section 152). Further, the criteria used for the selection of material for examination must not be referable to an individual known to be in the British Islands (section 152). There are safeguards relating to the disclosure of material to overseas authorities (section 151) and the selection for examination of legally privileged material (section 153).

49. There are additional safeguards in relation to confidential journalistic material. Once the amendments come into force (see paragraph 9 above), the Investigatory Powers Commissioner must first approve the use of selection criteria where one of the purposes is to identify confidential journalistic information or to identify or confirm a source of journalistic information, or the use of such criteria would be highly likely to identify such material or source. In a written ministerial statement made to Parliament on 31 March 2022, the Secretary of State stated that prior internal authorisation for the use of what were called "strong selectors", that is, search terms linked to identifiable individuals (such as e-mail addresses) will be required.

50. Bulk interception warrants last for 6 months unless already cancelled. They may be renewed by a decision of the Secretary of State, taken personally, and with the approval of the Judicial Commissioner (section 144).

51. There is provision for supervision and oversight of these powers in Part 8. The arrangements are described below. There are provisions for applications to an Investigatory Powers Tribunal ("IPT") which are also described below.

Part 6 Chapter 2 - Bulk Acquisition Warrants

52. A bulk acquisition warrant is a warrant requiring a telecommunications operator to obtain and/or disclose any communications data specified in the warrant (section 158(5)-(6)). The power is limited to communications data. That is defined as data about a person or thing (entity data) and data which defines an event on or by means of a telecommunication system (events data). In very broad terms, it covers data about who was using a telecommunications system and where and when. It does not include the content of communications (section 261).

53. The arrangements governing these warrants are broadly similar to the arrangements described above in relation to bulk interception warrants. In brief, the warrant must be necessary in the interests of national security (alone or together with prevention or detection of serious crime or the economic well-being of the United Kingdom so far as relevant to national security) (section 158). They must specify the operational purpose for which any communications data may be selected for examination (section 161). The warrant may only be applied for by or on behalf of the head of an intelligence service and must be granted by the Secretary of State personally (sections 158(9) and 160). The Secretary of State must ensure that the warrant is necessary for the statutory purposes. The warrant must be approved by a Judicial Commissioner who must consider whether the warrant is necessary for the statutory purposes, that the conduct authorised is proportionate to what is sought to be achieved and that the examination of the communications data for each of the specified operational purposes is necessary (section 159). The Secretary of State must be satisfied that there are in force satisfactory arrangements governing the use and disclosure of data (section 171). They must ensure that the number of people to whom the material is disclosed and the extent to which it is made available and copied is limited to the minimum necessary (section 171). The arrangements must also ensure that data may only be selected for examination for the specified operational purposes and so far as that is necessary and proportionate (section 172). Warrants cease to have effect after six months (section 162). The oversight arrangements in Part 8, described below, and the provisions for applications to the IPT, apply to the exercise of functions governing bulk acquisition warrants.

Part 6 Chapter 3 - Bulk Equipment Interference Warrants

54. Bulk equipment interference warrants authorise the interference with any equipment for the purpose of obtaining communications, equipment data and other information. Their main purpose must be to obtain overseas-related communications, information or equipment data. Such a warrant may also authorise the selection for examination of any material obtained under the warrant and the disclosure of such information (section 176).

55. The arrangements governing these warrants are similar to the arrangements governing bulk interception warrants. In brief, the warrant must be necessary in

the interests of national security (alone or together with prevention or detection of serious crime or the economic well-being of the United Kingdom so far as relevant to national security) (section 178). They must specify the operational purpose for which any material obtained under the warrant may be selected for examination (section 183). The warrant may only be applied for by or on behalf of the head of an intelligence service and must be granted by the Secretary of State personally (section 178(4) and 182). The Secretary of State must ensure that the warrant is necessary for the statutory purposes. The warrant must be approved by a Judicial Commissioner who must consider whether the warrant is necessary for the statutory purposes, that the conduct authorised is proportionate to what is sought to be achieved and that the examination of the material for each of the specified operational purposes is necessary (section 179). There are provisions requiring the Secretary of State to ensure that there are arrangements in force governing the use and retention of such material (section 191). Those arrangements must ensure that the number of people to whom the material is disclosed and the extent to which it is made available and copied is limited to the minimum necessary (section 191). Those arrangements must also ensure that selection of data for examination may only be carried out for the operational purposes specified in the warrant and if that is necessary and proportionate. Further, data must not be selected for examination if any of the criteria used for selection are referable to an individual known to be in the British Islands (section 191 and 193). Warrants cease to have effect after six months (section 184). The oversight arrangements in Part 8, described below, and the right of application to the IPT apply to the exercise of functions governing bulk equipment interference warrants.

Parts 3 and 4 – Retention Notices and Authorisations to Obtain Communications Data

56. Parts 3 and 4 of the Act deal with the retention and acquisition of communications data. They do not relate to the content of communications.

57. Part 4 deals with retention. Section 87 of the Act provides for the Secretary of State to issue a retention notice to a telecommunications operator to retain communications data. Such notices may be given where the Secretary of State considers retention necessary and proportionate in the interests of one or more of the following purposes: national security, prevention or detection of serious crime or crime (for communications data relating to events, and entities respectively), economic well-being of the United Kingdom so far as relevant to national security, public safety, prevention of death or injury, or investigation of alleged miscarriages of justice. A notice cannot require data to be retained for more than 12 months. Section 87(2) provides that a retention notice may:

> "(a) relate to a particular operator or any description of operators,
>
> (b) require the retention of all data or any description of data,
>
> (c) identify the period or periods for which data is to be retained,

> (d) contain other requirements, or restrictions, in relation to the retention of data,
>
> (e) make different provision for different purposes,
>
> (f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice."

58. A Judicial Commissioner must approve the decision to issue a retention notice and must consider whether the notice is necessary and proportionate for the purposes for which it is sought. A Judicial Commissioner must also consider the matter with a sufficient degree of care to ensure that he or she complies with the general obligations relating to the protection of privacy set out in section 2 of the Act (section 89). There are obligations on a telecommunications operator to maintain the integrity and security of communications data which it is required to retain under the Act (section 92) and to put in place adequate security arrangements to prevent unauthorised disclosure (section 93).

59. Part 3 of the Act deals with authorisations for obtaining data that has been retained. Section 60A of the Act empowers the Investigatory Powers Commissioner to authorise a relevant public authority to obtain the communication data where he or she considers:

> "(a) that it is necessary for the relevant public authority to obtain communications data for a purpose falling within subsection (7),
>
> (b) that it is necessary for the relevant public authority to obtain the data—
>
> (i) for the purposes of a specific investigation or a specific operation, or
>
> (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and
>
> (c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved."

60. The purposes for which communications data may be obtained are those for which a retention notice may be issued and are described in paragraph 26 above, together with one additional purpose, the identification of a dead person or a person who is unable to identify himself or herself because of a mental or physical condition (section 60A(7)). There are restrictions on the circumstances in which the Investigatory Powers Commissioner can authorise the obtaining of data which can only be obtained by processing an internet connection record. The Investigatory Powers Commissioner cannot grant such authorisations to

local authorities and, in relation to other public authorities, the purposes for which that data may be obtained are restricted to the interests of national security or the prevention or detection of serious crime and the Investigatory Powers Commissioner considering that it is necessary to obtain the data to identify which person or apparatus is using an internet service (section 62). Authorisations last for one month (section 65). There are additional powers for designated senior officers of certain public authorities to grant authorisations (sections 61 and 61A).

61. The oversight arrangements in Part 8, described below, and the provisions for application to the IPT, apply to the retention and acquisition of communications data under Parts 3 and 4 of the Act.

Part 5 – Targeted Equipment Interference Warrants

62. The warrants that may be issued under Part 5, and which are in issue this appeal, are targeted equipment interference warrants. That is a warrant which authorises a person to secure interference with any equipment for the purpose of obtaining communications, equipment data and any other information, including by monitoring, observing or listening to a person's communications and recording them (section 99). The subject matter of targeted equipment interference warrants is defined in section 101 of the Act as follows:

> "101 Subject-matter of warrants"
>
> (1) A targeted equipment interference warrant may relate to any one or more of the following matters—
>
> (a) equipment belonging to, used by or in the possession of a particular person or organisation;
>
> (b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
>
> (c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
>
> (d) equipment in a particular location;
>
> (e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;
>
> (f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;
>
> (g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference

> with equipment for the purpose of obtaining communications, equipment data or other information;
>
> (h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment."

63. The applications under section 102 must be made by or on behalf of the head of an intelligence service. The Secretary of State may only issue a warrant if it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom (so far as those are relevant to the interests of national security). The Secretary of State must consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved (section 102). The Secretary of State must also ensure that there are arrangements in place for limiting the number of persons to whom material is disclosed, the extent to which any material is disclosed, and the extent and number of any copies (sections 102(1)(c) and 129). If one of the purposes is to obtain items subject to legal privilege, that must be stated in the application and the warrant; and the Secretary of State must have regard to the public interest in the confidentiality of legally privileged material and may only grant the warrant if there are exceptional and compelling circumstances which make it necessary to authorise such interference and there are arrangements in place relating to the disclosure and retention of such material (sections 112 and 129). If one of the purposes of the warrant is to obtain confidential journalistic material or to identify or confirm a source of journalistic information, that must be stated in the application for a warrant and the Secretary of State may only issue the warrant if there are arrangements in place relating to the disclosure and retention of such material (sections 112, 113 and 129). The details that must be specified in the warrant are set out in section 115 of the Act. There are also detailed provisions governing warrants granted on the application of the Chief of Defence Intelligence and law enforcement officers (sections 104 to 107). In addition, under section 106, applications may be granted by law enforcement chiefs on the application of an appropriate officer to them (with Judicial Commissioner approval).

64. A Judicial Commissioner must approve the decision to issue a targeted equipment interference warrant. The Judicial Commissioner must consider whether the warrant is necessary and whether the conduct authorised is proportionate (section 108).

65. The oversight arrangements in Part 8, and the provisions for application to the IPT, apply to the exercise of functions related to the issuing of targeted equipment interference warrants.

Part 7 – Bulk Personal Datasets

66. The provisions in Part 7 authorise the retention and examination of bulk personal datasets which the intelligence services have already acquired under

other statutory provisions. Section 200 of the Act provides that an intelligence service may not exercise a power to retain or examine a bulk personal dataset unless that is authorised by a warrant issued under Part 7. The intelligence services retain a bulk personal dataset if they have acquired a set of information, including personal data within the meaning of section 3(2) of the Data Protection Act 2018, relating to a number of individuals, 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 services, the intelligence services retain the set and the set is held or to be held electronically for analysis.

67. There are two types of warrants that can be issued under Part 7. First there are class bulk personal dataset warrants, applicable to a class of bulk personal datasets, and second, specific bulk personal dataset warrants. In both cases, an application is made by or on behalf of the head of an intelligence service and an application must be granted by the Secretary of State personally (sections 204 and 205). The Secretary of State may only issue either type of warrant if he or she considers it necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as relevant to the interests of national security and that the conduct authorised is proportionate (sections 204 and 205). An application must specify the operational purpose or purposes which are to be included in the warrant (if any) (sections 204(2) and 205(4)). The Secretary of State must consider that examination of the relevant bulk personal datasets is necessary for each of the specified operational purposes (sections 204(3)(c) and 205(6)(c)). The Secretary of State must consider that the arrangements for storing bulk personal datasets and preventing unauthorised disclosure are satisfactory.

68. There are specific restrictions on the use of protected data. For present purposes, protected data, essentially, comprise the content of communications (save that systems data, which might include certain types of data which include content, namely data enabling or facilitating the function of a telecommunication system or service, and information which is not private information are not protected data). Class bulk personal dataset warrants cannot authorise the retention or examination of protected data (section 202). Where a specific bulk personal dataset warrant is issued, the Secretary of State may impose conditions governing the selection for examination of protected data on the basis of criteria referable to an individual known to be in the British Islands. There are also restrictions on the issuing of a specific bulk personal dataset warrant if the purpose is to authorise the retention and examination of health records. The Secretary of State may only issue a specific bulk personal dataset warrant if there are exceptional and compelling circumstances that make it necessary to authorise the retention or examination of health records.

69. A Judicial Commissioner must approve the decision to issue a class or a specific bulk personal dataset warrant. The Judicial Commissioner must consider whether the warrant is necessary for the stated purpose, whether the conduct authorised is proportionate, and whether examination of the bulk personal dataset, or the class of bulk personal datasets, described in the warrant is necessary for each of the specified operational purposes (section 208).

70. The oversight arrangements in Part 8, and the provisions for application to the IPT, apply to the exercise of statutory functions in relation to bulk personal datasets.

Oversight Arrangements and Applications to the IPT

71. Part 8 of the Act provides for the oversight of the exercise of statutory functions. There is provision for the Investigatory Powers Commissioner to keep the exercise of functions relating to the interception of communications, the acquisition or retention of communications data, and equipment interference under review by way of audit, inspection and investigation (section 229). The Investigatory Powers Commissioner must make an annual report to the Prime Minister about the carrying out of the functions of Judicial Commissioners. This must include statistics on the use of investigatory powers, the results (including the impact) of such use, information about the operation of the safeguards in relation to legally privileged material, confidential journalistic material and sources. Copies of those reports must be sent to the Intelligence and Security Committee of Parliament. That Committee may refer matters to the Investigatory Powers Commissioner with a view to it being subject to investigation, inspection or audit (sections 234 and 236).

72. The IPT is created by section 65 of RIPA. The IPT has jurisdiction to hear complaints by persons aggrieved by the conduct of the intelligence services, or conduct for or in connection with the interception of communications. It is the sole appropriate tribunal for the purposes of section 7 of the HRA, that is, determining whether conduct by the intelligence services amounts to a violation of a Convention right.

The Convention Judgment

73. As noted above, because the Convention Judgment was given before the decision of the Grand Chamber in *Big Brother Watch* we do not have the benefit of the Divisional Court's views on its implications for the issues that arise in this appeal (materially for present purposes in relation to Grounds 1 to 3). The Divisional Court's analysis is nevertheless valuable in the following respects.

74. First, the Divisional Court identified that the real focus of the claim for judicial review was that the Act did not contain sufficient safeguards against the risk of abuse of discretionary powers. The claim did not allege that the provisions of the Act were not necessary or were not proportionate (paragraphs 154 to 156 of the Convention Judgment). Instead, it sought to obtain a declaration of incompatibility on the basis that the Act did not satisfy the requirement that any interference with the rights guaranteed by Article 8 had to be "in accordance with law" or prescribed by law for the purposes of Article 10.

75. Secondly, in the context of challenges to the bulk interception powers, as the Divisional Court observed at paragraph 160:

> "…the question of compatibility with the Convention must be determined by reference to the totality of the

> interlocking safeguards applicable at the various stages of the bulk interception process".

76. Thirdly, the Divisional Court drew attention to the significant differences between the statutory regime set out in the Act on the one hand and section 8(4) of RIPA on the other. In relation to bulk interception warrants, for example, the Divisional Court identified a number of relevant features of the Act which differed from RIPA: see paragraphs 142 to 151 of the Convention Judgment. Further, the Divisional Court emphasised that the Act, unlike RIPA, did require prior approval by an independent body of the decision to issue the warrant (the so called "double-lock"). At paragraph 149 to 151, the Divisional Court said this:

> "149. Very importantly, in our view, the warrant must also be authorised by a [Judicial Commissioner]. As we have already seen [Judicial Commissioners] must be persons who hold or have held a high judicial office, in other words at least a High Court judge. The IPC himself is currently a serving Lord Justice of Appeal.
>
> 150. The requirement for approval of a warrant by a JC is part of the so called "double-lock" system which the 2016 Act introduced. There was no such system under previous legislation such as RIPA, which was the subject of the judgment of the First Section in *Big Brother Watch*.
>
> 151. Furthermore, as is apparent from the overview at paras 109-120, the [Judicial Commissioners] have a number of other important functions, including oversight by way of audit, inspection and investigation. In our view, these are important safeguards which have been introduced by the 2016 Act. They are to be seen as part of the overall, interlocking structure which the Act has created."

77. It was against that background that the Divisional Court considered whether the totality of the safeguards provided under the Act in respect of the different powers conferred by the different parts of the Act were compatible with the Convention and found that the legislation was not incompatible with the Act (a conclusion that the appellant now contends is not consistent in certain respects with the observations of the Grand Chamber in *Big Brother Watch*).

78. Fourthly, the Divisional Court considered issues about which the Grand Chamber did not make any observations, and which now form the subject matter of Grounds 4 and 5 of the appeal.

79. Ground 4 concerns the claim that Part 7 of the Act, which deals with the retention of bulk personal datasets, is "impermissibly wide" so that the circumstances in which a bulk personal dataset warrant may be issued are not foreseeable and therefore not in accordance with law.

80. The Divisional Court identified the features, and the legal safeguards applying to bulk personal datasets at paragraph 214 to 219 of the Convention Judgment in the following terms:

> "215. The decision to issue either a class BPD warrant or a specific BPD warrant must be taken by the Secretary of State personally (section 211) and is subject to prior approval by a [Judicial Commissioner], except where the Secretary of State considers there is an "urgent need" for a specific BPD warrant to be issued (sections 204(3)(e), 205(b) (e) and 208). Where a specific BPD warrant is issued without prior [Judicial Commissioner] approval because of urgent need, the Secretary of State must inform a [Judicial Commissioner] that the warrant has been issued and, within three working days, the [Judicial Commissioner] must decide whether or not to approve that decision. In the event of a refusal to approve the warrant, it ceases to have effect (section 209). The [Judicial Commissioner] may direct the destruction of data retained under the warrant or impose conditions as to the use or retention of such data (section 210).
>
> 216. A class BPD warrant authorises the retention or examination of any BPD falling within a class described in the warrant; whereas a specific BPD warrant authorises the retention or examination of any BPD described in that document. Neither type of BPD warrant may be issued (or approved) unless both the Secretary of State and the JC consider that it is necessary on the grounds of national security, for the prevention or detection of serious crime, or in the interests of the economic well-being of the UK in so far as those interests are also relevant to national security. They must also be satisfied that the operational purposes specified in the application for the warrant are purposes for which examination of the BPD described is or may be necessary, and that such examination is necessary on any of the grounds upon which the warrant is considered necessary. In addition, both the Secretary of State and the [Judicial Commissioner] must be satisfied that the conduct authorised by a warrant would be proportionate to what is sought to be achieved (see sections 204(3), 205(6) and 208(1) and (2)).
>
> 217. Furthermore, the general duties in relation to privacy in section 2 are engaged. Thus, the Secretary of

> State and the [Judicial Commissioner] must consider whether what is sought to be achieved by the warrant could be achieved by other less intrusive means. They must also consider any aspect of the public interest in the protection of privacy (section 2(2)) and any consideration relevant to proportionality (section 2(3) and (4)). The [Judicial Commissioner] must consider these matters with a sufficient degree of care as to ensure that he or she complies with the duties under section 2 (section 208(2)(b)).
>
> 218. Thus, the issuing of BPD warrants under Part 7 is subject to many of the fundamental safeguards in Part 6 to which we have already referred, including, in particular, the "double-lock" provisions.
>
> 219. Furthermore, a BPD may not be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of or includes, "protected data" or "health records" (section 206) or that a substantial proportion of the BPD consists of "sensitive personal data". Essentially, "protected data" means (section 203) "private information" (which "includes information relating to a person's private or family life" and all other data in a BPD other than "systems data" or "identifying data" which is capable of being separated logically from that BPD without revealing the meaning of any of the data). An application to retain, or to retain and examine, data within these categories would have to be made as an application for a specific BPD warrant. Additional safeguards in relation to specific warrants covering "health records" and "protected data" are provided by sections 206 and 207 (see the overview at para 90)."

81. At paragraphs 223 to 227, the Divisional Court summarised the basis of the challenge in relation to bulk personal datasets and its conclusion in the following terms (references omitted):

> "223. At the outset of the hearing before us [counsel for the claimant] submits that the BPD powers conferred by Part 7 are too wide to be compatible with articles 8 and 10 because virtually any data could be retained and examined under a BPD warrant so long as it comprises personal data held electronically: paras 106-109 of the claimant's skeleton argument. By way of example, he said that the language of the legislation is so broad to allow the authorisation of the kind of national DNA or fingerprint data base which was held to be unlawful in *S*

and Marper and *MK v France* …. He submits that the safeguards relate solely to examination and not to the authorisation of retention.

224. We do not accept these submissions. As we have already indicated, the question for this court is whether the *legislation* as enacted, and not actual practices or activity, is incompatible with articles 8 or 10. Here the key issue for us is whether the legislation indicates the scope of the powers conferred and the manner in which they may be exercised with sufficient clarity to give adequate protection against "arbitrary interference": *Zakharov*, at para 230. The statutory requirement that both the Secretary of State and the independent [Judicial Commissioner] have to apply necessity and proportionality tests to a properly formulated application is designed to ensure that retention of the kind which was found to be in breach of the ECHR in *S and Marper* or in *MK* would not be authorised and would therefore be prohibited by section 200. Our conclusion is similar to that which we reached on the challenge regarding the general and indiscriminate retention of data under Part 4 of the 2016 Act (see *R (National Council for Civil Liberties) v Secretary of State for the Home Department* [2019] QB 481, para 135). It is wrong as a matter of principle to argue that Part 7 is incompatible with articles 8 and 10 by advancing factual scenarios which would be incompatible with legal principles (and independent mechanisms to give effect to those principles) enshrined in the Act itself.

225. We have reached a similar conclusion on the claimant's related argument that the legislation gives the Secretary of State a choice as to whether to issue a warrant for the retention of a BPD either in the form of a class BPD warrant or a specific BPD warrant. A class warrant is simply required to describe the class of BPD to which it relates without saying how a "class" is to be defined: para 115 of the claimant's skeleton argument. We agree with the defendants that if on a given set of facts it is not necessary or proportionate to issue a class BPD warrant because a less intrusive specific BPD warrant could be issued to address the purpose of the application, then neither the Secretary of State will be able to issue, nor a JC to approve, the issuing of a class BPD warrant…

226. This conclusion is reinforced by paras 5.3-5.5 of the BPD Code of Practice. If the [Judicial Commissioner] or the Secretary are not satisfied as to the nature and scope

> of a class, or the number of BPDs which may fall within the class, the application for a class warrant may be refused or it may be granted subject to conditions which reduce the ambit of the class. Alternatively, the intelligence service may be required to split the class for which a warrant is sought and to submit revised applications for smaller class BPD warrants so as to ensure effective oversight. Such outcomes are the direct result of applying the necessity and proportionality tests embedded in the statutory framework and machinery for the authorisation of warrants.
>
> 227. As we have previously explained, Part 7 neither authorises an agency to *obtain* data, nor to *retain* data which could not otherwise be retained under other legislation. Instead, it requires the retention of BPD previously obtained under other regimes to be subjected to the safeguards introduced by Part 7, not least the "double lock provision", requiring independent scrutiny and approval through the warrant procedure, and the subsequent monitoring of the audit process of the powers used. As the defendants point out, there is no challenge before the court to the regime in the ISA or the Security Service Act 1989."

82. The fifth ground of appeal concerns the adequacy of the safeguards in relation to legally privileged material.

83. The Divisional Court described the safeguards in relation to bulk interception warrants and bulk equipment interference warrants in Chapters 1 and 3 of Part 6 in the following terms at paragraphs 276 to 278 of the Convention Judgment:

> "276. Under the first safeguard, where a purpose of the criteria to be used for selecting such material for examination is to identify items subject to legal privilege, or the use of those criteria is likely to reveal such items, a "senior official" acting on behalf of the Secretary of State must approve the use of those criteria (sections 153(2) and 194(2)). That official must have regard to the public interest in the confidentiality of such items (section 153(3) and section 194(3)). No such approval may be given unless the official considers that the arrangements under section 150 or section 191 include safeguards for the handling, retention, use and destruction of such items. Additionally, where the purpose is to identify items subject to legal privilege, the official must be satisfied that there are "exceptional and compelling circumstances" making it necessary to authorise the use of those selection criteria (section

> 153(4) and section 194(4)). That test is not satisfied unless the official is satisfied that the public interest in the selection for examination outweighs the public interest in the confidentiality of "items" subject to legal privilege, there are no other means by which the information may reasonably be obtained, and the information is necessary for national security or to prevent death or significant injury (sections 153(5) and 194(3)).
>
> 277. Under the second safeguard, where a purpose of the criteria to be used for selecting "intercepted content" or "protected material" for examination is to identify communications that would be subject to legal privilege if they were not made in order to further a criminal purpose, those criteria may not be used unless approved by a senior official acting on behalf of the Secretary of State and that person considers that the targeted communications are likely to have been made with the intention of furthering a criminal purpose (sections 153(6)—(8) and 194(6)—(8)).
>
> 278. Under the third safeguard, where an item subject to legal privilege has been intercepted under Chapter 1 or obtained under Chapter 3 and is retained following its examination, other than to be destroyed, the IPC must be informed as soon as reasonably practicable (sections 153(9) and 194(9)). The IPC must either direct the destruction of the item or impose conditions on its use or retention (sections 153(10) and 194(10)), unless he considers that the public interest in retaining the items outweighs the public interest in the confidentiality of "items" subject to legal privilege and that retention is necessary for national security or for preventing death or significant injury (sections 153(12) and 194(12)). Even where he does so consider, the IPC may still impose conditions on the use or retention of the items in order to protect the public interest in the confidentiality of legal privilege (sections 153(11) and 194(11)). It is to be noted that the application of the third safeguard is not limited to "intercepted content" or "protected material"; it applies generally to any item subject to legal privilege which has been intercepted or obtained under Chapters 1 or 3 of Part 6."

84. The Divisional Court noted that similar provisions to those three safeguards for legally privileged material had been enacted in relation to specific bulk personal dataset warrants under Part 7 (paragraph 280). Further, the selection criteria referable to a person known to be in the British Islands could only be used with

the prior approval of a Judicial Commissioner (sections 222(2) and (4)). Provisions similar to the first two safeguards described above in relation to legally privileged material had also been enacted in relation to targeted equipment interference warrants under Part 5. Such warrants also require prior approval by a Judicial Commissioner.

85. Finally, the Divisional Court focussed on the oral submissions of counsel which criticised the absence of safeguards for legally privileged material in respect of the bulk acquisition of secondary data and non-protected data (under Chapters 1 and 3 of Part 6 and Part 7). The criticism involved assumptions that it may be possible to identify who has been communicating with whom from such data (and the further assumption, it seems, that such facts were legally privileged). There was further criticism of the lack of safeguards for the bulk acquisition of communications data (not content) under Part 2 of Chapter 6.

86. The Divisional Court dealt with these issues at paragraphs 285 to 292 in the following terms:

> "285. There was a dispute as to how exceptional or otherwise such examples of legal privilege may be. We do not need to resolve this. Even if legally privileged items falling outside the scope of "content" are intercepted or obtained under a warrant, they are subject to the "third safeguard" in section 153(9)—(14) and also sections 55 , 131 , 194(9)-(14) and 223 . The IPC must apply the dual tests of whether (a) the public interest in retention outweighs the public interest in the confidentiality of legally privileged items and (b) retention is necessary for national security or for preventing death or significant injury. Subject to the outcome of the IPC's assessment applying those tests, the commissioner may direct destruction of the items in question or the imposition of conditions on their retention or use.
>
> 286. The requirement under that third safeguard for both tests to be applied, if a legally privileged item is intercepted or obtained, also meets in substance the claimant's criticism that the first safeguard does not require those tests to be applied where the use of selection criteria for examination is only "likely to identify" legally privileged items, as opposed to its being a purpose of using those criteria to identify such items. In this context, we also bear in mind the overarching requirements of the general duties in relation to privacy, notably section 2(2)(a)(b) and (d), (4)(c) and (5). These protections under the third safeguard are not confined to "content", "protected material" or "protected data" but apply also to "secondary data" and to non-protected material or data.

287. The claimant also criticises this third safeguard because it does not provide for prior independent authorisation of the interference. We accept the submission of Sir James Eadie [counsel for the Secretary of State] that neither Strasbourg nor domestic jurisprudence lays down a general requirement for such authorisation in order to achieve compatibility with article 8 in relation to legally privileged items: see *McE v Prison Service of Northern Ireland (Northern Ireland Human Rights Commission intervening)* [2009] AC 908; *RE v United Kingdom* (2015) 63 EHRR 2; *Szabo v Hungary* (2016) 63 EHRR *3*; *Michaud v France* (2012) 59 EHRR 9.

288. We do not accept that the claimant's contention is supported by the decision in *Kopp v Switzerland* (1998) 27 EHRR 91. There the Federal Prosecutor had ordered monitoring of the private and professional phone lines of a lawyer and his wife, who was the former head of the Federal Department of Justice and Police, in order to identify a person working in that department who might have disclosed official secrets. The monitoring covered all the telephone lines in the lawyer's office and therefore also involved listening to privileged communications by all the lawyers in the office. In those unusual circumstances, the court expressed concern that the task of distinguishing between calls that were the subject of the investigation and other calls, the contents of which were legally privileged, had been entrusted to an official in the legal department of the Post Office without supervision by an independent judge. However, the court did not lay down any general principle requiring prior authorisation by a judge or other independent body of the interception or obtaining of material which is the subject of legal privilege.

289. The claimant criticises Part 7 of the 2016 Act for failing to apply the safeguards in respect of legally privileged items to "class" BPD warrants. However, we accept the defendants' submission that such items will fall within the definition of "protected data" (section 203). In this context it should be recalled that "identifying data" which is incapable of being separated logically from BPD without revealing the meaning of any of the data is treated as "protected data". By section 202 an intelligence service may not retain, or retain and examine, BPD which includes protected data. In such circumstances, it will be necessary for a "specific" BPD warrant to be obtained and the safeguards in respect of legally privileged items will apply.

> 290. As for the claimant's criticism that Chapter 2 of Part 6 does not contain specific safeguards in relation to the bulk acquisition of CD, we have previously referred to the general privacy duties in section 2 and the relevant parts of the Code of Practice. The case law upon which the claimant relies (cited above) is all concerned with the targeted surveillance of the content of lawyer-client communications, not the obtaining or examination of CD. That case law does not lay down a lexicon of specific rules for surveillance of any lawyer-client communication. Instead, it refers to a broad principle that the importance of lawyer-client confidentiality requires specific recognition in domestic legal rules. Beyond that principle the issue of whether additional protection is required depends upon the context. That broad principle is reflected in section 2 of the 2016 Act.
>
> 291. Furthermore, as we have explained, "content" is excluded from the ambit of CD (section 261(5)). Indeed, the legislation goes further by excluding from the ambit of CD anything within the scope of "systems data" which would otherwise fall to be treated as "content". Thus, the acquisition, examination and disclosure of "content" cannot be authorised by a warrant issued under Chapter 2 of Part 6. We accept the defendants' submission that, although CD may reveal when a communication occurred, between which devices, and for how long, it will not reveal what was discussed or the subject matter. It will not therefore touch upon the central purpose of legal privilege, namely to enable a client to disclose whatever he wishes to in order to obtain legal advice, without the fear of that material being disclosed to others without his consent.
>
> 292. For all these reasons we are satisfied that the rules regarding legally privileged items are set out in the 2016 Act and codes of practice with sufficient clarity and with sufficient safeguards so as to avoid arbitrary interference and so as to render the statutory scheme compatible with article 8."

87. For those reasons, the Divisional Court held that the provisions of Parts 3, 4, 5, 6 and 7 were not incompatible with Articles 8 and 10 of the Convention.

88. The Divisional Court also considered, and rejected, five specific arguments concerning the scope of the definitions used in connection with safeguards relating to journalistic material (paragraphs 340 to 352 of the Convention Judgment).

The first and second EU law judgments

The Issues of Retained EU Law

89. The issues of retained EU law have their origin in Directive 2002/38/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the Directive") and provisions of the Charter. Article 5 of the Directive provides that Member States shall ensure the confidentiality of communications and related traffic and, in particular, shall prohibit, amongst other things, interception or surveillance of communications and related traffic data.

90. Article 15 of the Directive, however, permits Member States to adopt legislative measures when such restrictions constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security.

91. Article 8 of the Charter guarantees that everyone has the right to protection of personal data concerning him or her. Article 7 of the Charter guarantees to everyone the right to respect for his or her private and family life, home and communications. Article 11 of the Charter guarantees the right to freedom of expression. These later two articles correspond to Articles 8 and 10 of the Convention, respectively. Article 52 of the Charter provides that any limitation on the exercise of the rights recognised by the Charter must be provided by law and must be necessary. Article 52.3 of the Charter provides that:

> "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

92. The Act was adopted, and the claim for judicial review issued, at the time when the United Kingdom was a member of the European Union. The provisions of the Directive were therefore capable of being directly effective in United Kingdom law by virtue of section 2 of the European Communities Act 1972 ("the 1972 Act"). The Charter was also part of the law of the United Kingdom at that stage by virtue of the 1972 Act. The United Kingdom left the European Union on 31 January 2020 and the 1972 Act was repealed. There then followed an implementation period during which European Union Law continued to be part of the law of the United Kingdom. That period ended on 31 December 2020.

93. However, Parliament provided that any rights or remedies formerly arising under the 1972 Act (such as a directly effective right derived from a European Union Directive) remained available in domestic law (section 4 of the European

Union (Withdrawal) Act 2020 (the 2020 Act)). The Charter ceased to be part of the law of the United Kingdom save that Parliament enacted that the Charter continued to apply in relation to proceedings started before the end of the implementation period (section 5(4) and paragraph 39(3) of Schedule 8 to the 2020 Act). By that route, as the Divisional Court recognised, the provisions of the Directive and the Charter remain relevant to this claim (paragraphs 28 to 37 of the second EU Judgment).

94. Against that background, three issues of retained EU law were considered by the Divisional Court and are now raised on this appeal.

95. The first concerns decisions of the CJEU that Article 15 of the Directive must be read as precluding national legislation which, for the purpose of preventing or detecting crime, provided for the general and indiscriminate retention of all data: see Joined Cases C-203/15 and C-698/15 *Tele2Sverige AB v Post-och telstyrelsen* and *Watson*.

96. In the first EU Judgment, the Divisional Court considered, amongst other questions, whether Part 4 of the Act involved the general and indiscriminate retention of data. It observed that the categorisation had been applied to Swedish legislation in the *Tele2Sverige* case heard with the *Watson* case. That legislation required all providers of electronic communications to retain all data. The requirements of the legislation were not qualified by a necessity or a proportionality test. The Divisional Court considered that Part 4 of the Act was different for seven reasons set out at paragraphs 127 to 134:

> "127. The scheme laid down in Part 4 of the 2016 Act is very different from the Swedish legislation. First, the Act does not contain a blanket requirement requiring the general retention of communications data. The Act does not itself impose any requirement on telecommunications operators to retain data. Instead, the Secretary of State is given a power to require retention of data by serving a notice on an operator.
>
> 128. Secondly, the Secretary of State may only exercise that power if she considers it both necessary and proportionate for one or more of the specific purposes currently listed in section 61(7) of the Act. This enshrines in the statute the essence of the tests propounded by the court in *Watson CJEU*.
>
> 129. Thirdly, although the claimant relies heavily upon section 87(2)(b) as allowing a notice to require the retention of "all data", that provision cannot be read in isolation and taken out of its context. The claimant's submission overlooks the statutory requirement to satisfy the necessity and proportionality tests. It is difficult to conceive how a retention notice drafted so as to encompass all communications data in the UK could satisfy those tests. In any event, section 87(2) provides

that a notice may relate to a "description of data" and not just to "all data". Furthermore, a notice may relate to a particular operator or to a description of operators. These and the other matters specified in section 87(2) must be read as a whole. Taken together they simply list the elements which may be used when delineating the content and scope of a retention notice so as to satisfy the necessity and proportionality tests in any particular case.

130. Fourthly, although a retention notice may specify the period of time for which data is to be retained (section 87(2)(c), that period may not exceed 12 months: section 87(3).

131. Fifthly, before the Secretary of State may serve a retention notice, she must have regard to, among other matters, the factors listed in section 88(1), which comprise the likely benefits of serving the notice, the number of users to which the notice relates, the technical feasibility and costs of complying with the notice and any other effect on the telecommunications operator to be served. In addition, before serving a retention notice the Secretary of State must also take reasonable steps to consult any operator to whom the notice will relate: section 88(2).

132. Sixthly, by section 87(1)(b) a retention notice may not be given unless the Secretary of State's decision has been approved by a Judicial Commissioner under section 89…..

133. In deciding whether to approve a retention notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the requirements in the proposed notice are necessary and proportionate for one or more of the purposes in section 61(7): see section 89(1). In performing this function, a commissioner must apply the same principles as would be applied by a court in an application for judicial review and ensure that his or her consideration is sufficiently careful so as to comply with the duties in section 2 of the Act. By section 2(2) a commissioner 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."
>
> The reference in section 2(2)(b) to "sensitive information" includes items subject to legal privilege and any information identifying a source of journalistic information: section 2(5). By section 2(4) a commissioner may also have regard to any other consideration relevant to whether the proposed notice is *necessary* for one of the statutory purposes and is *proportionate*, and the requirements of the HRA and of public law.
>
> 134. Seventhly, a telecommunications operator which receives a retention notice may refer the notice back to the Secretary of State for a formal process of review in accordance with sections 90 to 91. When these provisions are fully in force the Secretary of State will have to consult and take into account the report of a body called the Technical Advisory Board and a Judicial Commissioner: section 90(6), (9)…and (10). The Secretary of State may not vary or confirm a notice (as opposed to revoking a notice) unless that decision is approved by the IPC: section 90(11)."

97. The Divisional Court concluded that Part 4 of the Act did not involve the general and indiscriminate retention of data. It summarised its conclusions in paragraphs 135 and 137 in the following way:

> "135. In the light of this analysis of the structure and content of Part 4 of the 2016 Act, we do not think it could possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data. The legislation requires a range of factors to be taken into account and imposes controls to ensure that a decision to serve a retention notice satisfies (inter alia) the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles.
>
> …..
>
> 137. Ultimately, the overall amount of data which is retained under Part 4 of the 2016 Act will be the outcome of applying a statutory regime which requires the contents of each retention notice to be necessary and proportionate….".

98. In the second EU Judgment, the Divisional Court later concluded that Part 3 of the Act did not provide for general and indiscriminate retention of data for eight reasons. These were set out at paragraphs 109 to 117 of the Second EU Judgment. The Divisional Court also rejected arguments that Parts 5 and 6 involved the general and indiscriminate retention of data as that term was used by the CJEU, as the analysis applicable to Part 4 applied to Parts 5 and 6 as well.

99. In relation to Part 7, the Divisional Court considered that Part 7 did not fall within the scope of EU law saying, at paragraph 139 of the Second EU Judgment that:

> "139. First, we accept the defendants' submission that Part 7 of the IPA does not fall within the scope of EU law at all. Part 7 does not contain any power to acquire information, still less impose a duty upon [communication service providers] to provide information to the state. Rather it concerns how state authorities should handle bulk personal datasets which they have already obtained under other powers. We do not accept Mr Jaffey's submission that, because the data will originally have been obtained under other powers from [communication service provides] that brings it within the scope of the e-Privacy Directive. We note, as the defendants do, that in the proceedings which led to the reference by the IPT in *Privacy International*, the claimant in that case conceded that, in the absence of a regime requiring controllers to provide bulk personal datasets to an agency, the regime was outside the scope of EU law; see also the judgment of the CJEU, at para 45–46."

100. The Divisional Court also considered an argument that parts of the Act did not require independent authorisation each time data was accessed for a purpose other than national security, save in limited circumstances, and that this was inconsistent with the *Watson* judgment. The Divisional Court rejected that argument at paragraph 145 of the second EU Judgment:

> "145. We accept the submissions for the defendants that *Watson CJEU* did not go so far as to require separate independent authorisation each time retained data is selected for examination or accessed. The requirement for independent authorisation is satisfied by the need for approval to be obtained from a Judicial Commissioner for a bulk warrant which addresses not only the obtaining of data but also access thereto. This is reinforced by the statutory safeguards, as summarised in the Annex to our 2019 judgment, at paras 42–65."

101. Finally, of relevance to this appeal, the Divisional Court considered an argument that, following the decision of the Grand Chamber in *Big Brother Watch*, the Act should be understood to be incompatible with the Convention in two specific respects and that the Charter should be interpreted and applied in the same way. In that regard, the Divisional Court noted that it had already given its judgment on the Convention issue (in the Convention Judgment) and that the view to be taken of the decision in *Big Brother Watch* was a matter for the Court of Appeal. In relation to EU law, the Divisional Court said the judgment of the Grand Chamber was not binding on the CJEU. Further, if any judgment of the CJEU were to adopt the reasoning of the Grand Chamber, that judgment would not be binding on the courts in the United Kingdom, although those courts could take it into account following the United Kingdom's departure from the European Union.

102. In those circumstances, the Divisional Court considered that the claimant could not rely on EU law as an indirect means of achieving compliance with the judgment of the Grand Chamber in *Big Brother Watch* (paragraphs 149 to 158 of the second EU Judgment).

The Appeal

103. For the purposes of this appeal, it is convenient to take the Grounds of Appeal in the following order. We deal first with Ground 2, so far as that concerns Parts 6 and 5 of the Act, as this ground involves a generalised challenge to the adequacy of the different Parts of the Act when measured against the Convention. We deal next with Grounds 1 and 3, 4 and 5 in so far as they challenge particular aspects of Parts 6, 3, 4 and 5 of the Act. We then turn to the challenges under Grounds 1 to 5 in so far as they concern Part 7. Finally, we deal with Grounds 6 to 8 as they raise discrete points relating to retained EU law.

The First Issue:

Ground 2: The Adequacy of Safeguards governing search terms in relation to Parts 5 and 6 of the Act

104. Mr Ben Jaffey KC, with Mr Heaton and Ms Bird, for the appellant, submits that three significant safeguards identified as necessary by the Grand Chamber in *Big Brother Watch* are absent in relation to Parts 5 and 6 of the Act. Consequently, the provisions are not in accordance with law for the purposes of Article 8, are not prescribed by law for the purposes of Article 10, and do not justify any interference with the rights guaranteed by those Articles.

105. First, Mr Jaffey submits that the Grand Chamber recognised that there was a need for the categories or types of selectors, or search terms, to be identified in the application for the warrant and there was no provision for that under the Act. Mr Jaffey relies on paragraphs 354 and 381 to 382 amongst others of the judgment in *Big Brother Watch*. He submits that the requirement in sections 142 and 183 (in Part 6 Chapters 1 and 3) that operational purposes be specified was insufficient for these purposes. That requirement simply set out the purpose for which a warrant could be granted at a greater level of specificity than the

grounds upon which a warrant could be granted. It was a subcategory of purpose, not a category of search terms. It did not describe the category of selectors or search terms that would be used for deciding whether material would be examined. Further, the specified operational purposes were no different in substance from the certificate that had to be provided previously under section 8(4) of RIPA and that had been found to be insufficient in *Big Brother Watch.* The same applied to Part 7. There was no requirement for the operational purposes to be specified for warrants issued under Part 5 of the Act.

106. Secondly, Mr Jaffey submits that the use of strong selectors, that is search terms linked to an identifiable individual to identify which material should be examined, required prior internal authorisation. The respondents had accepted that prior internal authorisation was required for strong selectors in relation to bulk interception warrants under Part 6 Chapter 1. However, the respondent had not accepted that that was required for the remainder of Part 6 or Part 5.

107. Finally, he submits that the absence of a safeguard preventing the examination of secondary data under Part 6 Chapter 1 which was referable to an individual in the British Islands was also a deficiency which resulted in Part 6 Chapter 1 failing to provide adequate safeguards. There was no objective and reasonable basis for the differentiation between content (where the safeguard applied) and secondary data (where it did not). The same applied to the differential treatment of protected data in relation to Part 6 Chapter 3. Content could not be examined if it is referable to a person in the British Islands but equipment data could. Such data could often include items such as a private diary or photographs stored on equipment (but not transmitted) and so accessible by a bulk equipment interference warrant. Similar criticisms were made of Part 5.

108. Sir James Eadie KC, with Mr Facenna KC, Mr Milford KC, Mr Armitage, Mr Bethell and Ms Kelleher for the respondents, submits that the Grand Chamber in *Big Brother Watch* had accepted that bulk interception powers fell within a state's margin of discretion. In order to determine if the legislation was in accordance with law, it was necessary to consider the totality of the safeguards. Further, as a general matter, *Big Brother Watch* concerned RIPA not the Act, which had different provisions and different, and strengthened, safeguards. It was not possible to read the observations of the Grand Chamber in the context of RIPA as being transferrable, or applicable, to the different Parts of the Act. Nor was it appropriate to treat the observations of the Grand Chamber made in the context, as it said, of "bulk interception powers" as applicable to other types of powers under different Chapters of Part 6, or different Parts of the Act.

109. In relation to bulk interception warrants in Chapter 1 of Part 6, Sir James submits that they were foreign focussed, concerning overseas communications. They had to be used in the interests of national security. Only heads of security intelligence agencies could apply. The Secretary of State must personally grant them. He or she had to be satisfied they were necessary and proportionate. Further, they had to specify the specific operational purposes for which the material could be examined. In addition, and significantly, there had to be prior approval by a Judicial Commissioner who had to be satisfied that the examination of material was necessary and proportionate for each specified operational purpose. It was possible through the use of specified operational

purposes to control the data that would be examined. Further, if the Judicial Commissioner was not satisfied, he could call for further information. Strong selectors would now require prior internal authorisation (as explained in the written ministerial statement). There were oversight arrangements and remedies before the IPT. In totality, therefore, the safeguards were sufficient to ensure that there was no risk of abuse. The legislation was in accordance with law.

110. So far as the other Chapters of Part 6 are concerned, Sir James submits that it is not possible to read across from the observations made in the context of bulk interception powers and to conclude that the safeguards referred to by the Grand Chamber for bulk interception powers applied to other powers. The same regime governing the assessment of the necessity of a warrant for the stated grounds applied. The Secretary of State and the Judicial Commissioner had to determine whether the examination of the relevant data was necessary for each specified operational purpose. The requirement that there be prior internal authorisation of the use of strong selectors could not be read across to other powers. In relation to Part 6 Chapter 2, the use of search terms against a set of communications data was not the equivalent to the use of strong selectors in relation to the content of individuals' communications which are being transmitted. Part 6 Chapter 3 was different as it was aimed at stored information, not the continuing transmission of communications, where the practicability of applying a requirement of prior internal authorisation of each search term was more difficult.

111. Further, Sir James submits that the fact that there was no British Islands safeguard in relation to secondary data or protected material in Part 6 Chapters 1 and 3 did not give rise to any incompatibility. The Grand Chamber accepted in *Big Brother Watch* that the fact that the British Islands safeguard applied differently as concerned content and communications data did not give rise to any deficiency.

112. Sir James submits that the powers governing targeted equipment interference warrants in Part 5 were different in kind from bulk interception powers and the totality of safeguards applied in relation to those powers was sufficient to ensure compliance with Articles 8 and 10 of the Convention.

Discussion and Conclusion on the First Issue

Preliminary Observations

113. By way of preliminary observation, the context in which the judgment in *Big Brother Watch* was given concerned the bulk interception of cross-border communications by the intelligence services. The Grand Chamber recognised that the threats faced by states and their citizens had increased. These threats included global terrorism, drugs trafficking, human trafficking and child exploitation. Many of the threats came from international networks of persons and organisations with access to increasingly sophisticated technology. The Grand Chamber considered that the decision to use a bulk interception regime to identify threats to national security or against national interests was one which fell within the range of choices open to a state (paragraphs 322 to 323 and 340). The Grand Chamber accepted that the bulk interception of

communications was "of vital importance to Contracting States in identifying threats to national security" (paragraph 424).

114. The use of such bulk interception powers could involve interference with the rights guaranteed by Article 8 and Article 10 and, in order to be justified, had to be in accordance with (or prescribed by) law. They had to have a basis in domestic law, and be foreseeable and accessible. In addition, and significantly, there had to be adequate and effective safeguards against the risk of abuse. In that context, the Grand Chamber recognised that the degree of interference with the rights guaranteed by Article 8 (or 10) would vary at different stages of the process. It was also aware that the bulk interception regimes did not all follow the same process or follow the same order. It identified the general approach to be taken to such issues. Then, when assessing the regime provided for by section 8(4) of RIPA, it considered the totality of the safeguards applied, and considered that, "viewed as a whole" the section 8(4) regime, despite its safeguards, "did not contain sufficient end-to-end safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse" (paragraph 425). In that context, it had identified certain fundamental weaknesses and considered that the safeguards applying to the section 8(4) RIPA regime "were not sufficient to counterbalance the shortcomings highlighted" (paragraph 425).

115. In that regard, the task for this Court is to consider the different regimes governing the different powers available under different Parts and Chapters of the Act. The Court will need to consider the degree of intrusion represented by the exercise of those powers, given the nature of the information to which they apply, and the stages of the process of surveillance. Against that background, the Court will need to assess the totality of the safeguards provided in relation to each set of powers, whether contained in the Act itself or in the relevant Code of Practice, to determine whether, viewed as a whole, the safeguards provided do adequately guard against the risk of abuse and whether they otherwise meet the requirements of having a basis in domestic law and are foreseeable and accessible or whether the absence of a particular safeguard or safeguards prevents that from being so.

116. It is also important to bear in mind the following. First, the provisions of the Act are different from those considered by the Grand Chamber in *Big Brother Watch*. Secondly, the judgment of the Grand Chamber needs to be read as a whole and in context. Care must be taken not to take statements within it out of context. Thirdly, domestic courts should be careful not to expand the scope of Convention rights unless they are fully confident that the European Court would reach the same conclusion on the interpretation and application of a Convention right.

117. This Court is concerned with ensuring that the obligations imposed by the HRA are respected. When questions arise in connection with Convention rights, as they do in this case, section 2(1) of the HRA requires domestic courts to take into account relevant judgments of the European Court of Human Rights. As the Supreme Court made clear in *R (AB) v Secretary of State for Justice* [2022] AC 487 at paragraphs 54 to 59, Parliament's purpose in enacting the HRA was to ensure that there is correspondence between the rights enforced domestically and those available before the European Court, not to provide for rights which

are more generous than those available before the European Court. In determining therefore whether the provisions of primary legislation can be interpreted in a way that is compatible with a Convention right or, if that is not possible, whether there should be a declaration that a provision of the Act is incompatible with a Convention right (sections 3 and 4 HRA), this court should be careful not to expand the scope of Convention rights as the Supreme Court said in *R (AB)* "further than [we] can be fully confident that the European Court would go".

Part 6 Chapter 1 – Bulk Interception Warrants

118. Against that background, we consider each set of powers in turn applying the eight criteria identified in *Big Brother Watch*. We deal first with bulk interception warrants in Chapter 1 of Part 6. First, the grounds upon which a bulk interception warrant may be issued are adequately set out in section 138 of the Act. They may only be used in in the interests of national security (either alone or together with the prevention of detection or crime or the economic well-being of the United Kingdom so far as relevant to national security). Secondly, the circumstances in which communications may be intercepted appear clearly from section 136 of the Act. A warrant may only be issued if the main purpose is the interception of overseas-related communications and secondary data. When conducting bulk interception, the authorities must use their knowledge of the way international communications work to identify those individual communication links that are most likely to contain overseas-related material (see the Code of Practice for the Interception of Communications ("the Interception Code")).

119. It is convenient to take the procedure for granting a warrant and the procedure for selecting, examining and using material (the third and fourth matters) together. The Interception Code prescribes the material to be included in the application for a warrant. That will include the background to the application, a description of the communications to be intercepted, a description of the conduct to be authorised, the operational purposes for which communications and secondary data may be selected and examined, consideration of whether the material may be made available to overseas authorities, a consideration of why the conduct to be authorised by the warrant is considered proportionate and why it could not be achieved by less obtrusive means and certain assurances. That material will, therefore, be available to the decision-makers. The decision must be made personally by the Secretary of State and the application for a warrant must be made by or on behalf of a head of an intelligence service.

120. The Secretary of State must be satisfied that the main purpose is to intercept overseas-related communications or to obtain secondary data from such communications and that the warrant is necessary in the interests of national security (together with one or both of the other two grounds if applicable). The warrant must set out the specified operational purposes for which material may be examined. The heads of the intelligence services must maintain a list of the operational purposes for which material may be examined. That list is subject to approval by the Secretary of State and the list is subject to review by the Prime Minister and provided to the Intelligence and Security Committee of Parliament. These were regarded as important safeguards by the Divisional

Court (paragraph 167 of the Convention Judgment). The operational purposes specified in the warrant must contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons (paragraph 6.62 of the Interception Code).

121. The need for the warrant to specify the operational purposes for which material may be examined will act as a significant constraint upon the use of search terms. The Secretary of State when issuing the warrant must be satisfied that each of the specified purposes is or may be a purpose for which the examination of material is necessary.

122. Further, the issuing of the warrant is subject to prior independent authorisation. The decision must be approved by a Judicial Commissioner who is a person who holds or has held high judicial office. The Judicial Commissioner must review the necessity for the warrant and whether the conduct authorised by the warrant would be appropriate. In addition, the Judicial Commissioner must consider when deciding whether to approve the decision to issue a warrant that each of the specified operational purposes is necessary *and* that "the examination of intercepted content and secondary data for each such purpose is necessary" (section 140(2) of the Act). The Judicial Commissioner is also required by the Act to have regard to whether what is sought to be achieved "could reasonably be achieved by less intrusive means" (section 2(2)(a) of the Act). The Judicial Commissioner will have all the information that the Interception Code prescribes be provided in the application for the warrant. The Judicial Commissioner may also seek further information and clarification and there is an obligation on others to provide such documents as the Judicial Commissioner may need (paragraph 6.29 of the Code and section 235 of the Act).

123. Furthermore, material cannot be selected for examination of intercepted content by the use of criteria referable to an individual known to be in the British Islands (section 152(4)). In addition, there is to be provision for prior internal authorisation of search terms linked to an identifiable individual (see the written ministerial statement).

124. We deal with the remaining three criteria briefly. There are provisions providing safeguards in relation to the storage and use of data (sections 150 and 152 described above). There are further provisions governing copying, storage and destruction in the Interception Code. A warrant lasts for six months (section 162). There are safeguards in relation to the disclosure of material to overseas authorities (section 151 of the Act). There are provisions for oversight and applications to the IPT.

125. The appellant submits that these provisions omit certain key safeguards. It relies on observations made by the Grand Chamber in *Big Brother Watch* in relation to RIPA and, in particular, the comments on the need for identification of the categories or types of search terms and the fact that the certificate issued under section 8(4) of RIPA was expressed in general terms and was insufficiently precise to provide any meaningful restriction (paragraph 387 of the judgment in *Big Brother Watch*). However, the position in relation to the Act is different. There is provision governing the selection of material for examination. This is

done at the stage of deciding to issue, or approve, the warrant. Both the grounds for issuing the warrant, and the restrictions for which material be selected for examination are dealt with at that stage. The fact that both matters are considered prior to issue is not, of itself, a deficiency. The Grand Chamber noted that bulk interception regimes may not all follow the same model and the different stages may not be discrete (paragraph 325 of its judgment).

126. We are satisfied that the need to specify operational purposes, the provision of information, and the obligation on both the Secretary of State and, in particular the obligation on the Judicial Commissioner to consider that each of the specified operational purposes is necessary and that the examination of data is necessary for each such purpose, does ensure a degree of control over the range of material that may be selected for examination. We are satisfied that, overall, the safeguards put in place do meet the underlying aims identified in the *Big Brother Watch* judgment in this regard, namely to ensure that there is adequate identification and control over the types or categories of selectors to be used. The safeguards in place, together with the need for prior independent authorisation and the duties on the Judicial Commissioner to consider necessity, proportionality and the question of whether the aims could be achieved by less intrusive means, fulfil essentially the same aim in this context. Furthermore, it is not for this court to determine which arrangements would be preferable.

127. The appellant also identifies a difference in relation to secondary data. That may be examined by using criteria referable to an individual who is in the British Islands (the content of communications cannot be examined by reference to such criteria). Secondary data includes identifying data (which is data which may, amongst other things identify a person using a system or service) and systems data (which means data enabling or facilitating the functioning of a system) (section 263 of the Act). The appellant gives individual examples of systems data (part of secondary data) which might, it submits, give information such as the websites the person was browsing which might give a picture of some of the activities of the person. As the Divisional Court held at paragraphs 172 to 178 of the Convention Judgment, as a general rule the examination of the most sensitive content raises greater privacy concerns than the examination of secondary data. The position in relation to the selection of secondary data for examination in relation to persons in the British Islands was not such as to lead to the conclusion that the legislative scheme established in relation to Part 6 Chapter 1 was incompatible with Convention rights. We agree.

128. In conclusion, therefore, we are satisfied that the totality of the safeguards in the legislation as amended and the Interception Code, do contain adequate and effective safeguards at each stage of the bulk interception process to guard against arbitrariness and abuse. The process from application for a warrant, approval of the issuing of the warrant and of the conduct specified, the controls over the examination of material, the arrangements for storage and use, together with a system of supervision and applications to the IPT, as described above do ensure adequate safeguards. They are based in domestic law, are accessible and foreseeable. The interference is therefore in accordance with law for the purposes of Article 8 of the Convention.

Part 6 – Chapter 2

129. Next we consider the power to issue bulk acquisition warrants. Such warrants authorise the operators to obtain and disclose any communications data. Communications data means entity data or events data. Entity data is data about a person and a thing, and any association between that person or thing and a telecommunications service. Events data means any data which describes an event (section 261 of the Act). In other words, these warrants do not authorise the interception of the content of communications. Rather they relate to facts relating to a communication, that is to matters such as "the who, when, where and how of a communication but not the content, i.e., what was said or written" (paragraph 2.8 of the Bulk Acquisition of Data Code of Practice (the "Bulk Communications Data Code").

130. The Grand Chamber recognised that such data could reveal personal information such as the identities and geographic location of the sender of communications and the equipment through which the communication was sent. Further, such intrusion may be magnified if obtained in bulk as they can be analysed so as to form a picture of a person (paragraph 342 of *Big Brother Watch*). However, it is right to note, as the Divisional Court did at paragraphs 172 to 178 of the Convention Judgment, that as a general rule the examination of the most sensitive content raises greater privacy concerns than the examination of secondary data. Furthermore, whilst the safeguards relating to the interception, retention and searching of communications will need to be considered by reference to the same safeguards applicable to the interception of content, the safeguards do not have to be identical (paragraph 416 of *Big Brother Watch*).

131. Against that background, the grounds upon, and the circumstances in which, a bulk acquisition warrant may be issued are adequately set out in section 158 of the Act. They may only be used in the interests of national security (either alone or together with the prevention or detection of serious crime or the economic well-being of the United Kingdom so far as relevant to national security). A warrant may only be issued to obtain communications data (that is, entity and events data as defined in section 263) for one of those purposes.

132. Paragraph 4.5 of the Bulk Communications Data Code prescribes the material to be included in the application for a warrant. That will include the background to the application, a description of the communications data to be acquired, a description of the conduct to be authorised, an explanation of why the acquisition of communications data in bulk is considered to be necessary for one of the statutory grounds which must always include an explanation of why it is necessary in the interests of national security, the operational purposes for which communications data may be selected for examination, consideration of whether the material may be made available to overseas authorities, an explanation of why the conduct to be authorised by the warrant is considered proportionate and why it could not be achieved by less obtrusive means and certain assurances. That material will, therefore, be available to the decision-makers.

133. The warrant must specify the operational purposes for which any communications data acquired under the warrant may be selected for examination (section 161 of the Act).

134. The Secretary of State when issuing the warrant must be satisfied that the warrant is necessary and the conduct which is sought to be authorised is proportionate. Furthermore, the Secretary of State must be satisfied each specified operational purpose is a purpose for which examination of communications data is or may be necessary and that the examination of communications data is necessary for each of the specified purposes (section 158). Decisions must be taken personally by the Secretary of State and the application made by or on behalf of a head of an intelligence service.

135. Further, the issuing of the warrant is subject to prior independent authorisation. A Judicial Commissioner must review the necessity for the warrant and whether the conduct authorised by the warrant would be proportionate. The Judicial Commissioner must consider whether each of the specified operational purposes is necessary *and* that "the examination of intercepted content and secondary data for each such purpose is necessary" (section 159 of the Act). The Judicial Commissioner is also required by the Act to have regard to whether what is sought to be achieved "could reasonably be achieved by less intrusive means" (section 2(2)(a) of the Act). The Judicial Commissioner will have all the information that the Interception Code prescribes should be included in the application for the warrant. The Judicial Commissioner may also seek further information and clarification and there is an obligation on others to provide such documents as the Judicial Commissioner may need (paragraph 4.15 of the Bulk Communications Data Code and section 235 of the Act).

136. There are safeguards in relation to the storage and examination of communications data (section 171 and section 9 of the Bulk Communications Data Code). Communications data may only be examined if necessary for a specified operational purpose and if proportionate (section 172 and paragraphs 6.12 to 6.15) Further, specific consideration must be given as to whether a higher degree of protection is required in relation to the acquisition of communications data by reason of the particular sensitivity of such information (section 2 of the Act and paragraphs 6.19 to 6.23 of the Bulk Communications Data Code). There are safeguards in relation to the disclosure of material to overseas authorities: see section 171 and sections 9.10 to 9.12 of the Bulk Communications Data Code). A warrant lasts for six months (section 162). There are provisions for oversight and appeal.

137. The totality of the safeguards governing bulk acquisition of communications data need to be viewed as a whole. We are satisfied that they do contain adequate and effective safeguards at each stage to guard against arbitrariness and abuse in relation to the level of intrusion represented by the acquisition of such communications data. The process from application for a warrant, approval of the issuing of the warrant and of the conduct specified, for the examination of material, for storage and use, together with a system of supervision and applications to the IPT, described above do ensure adequate safeguards.

138. The appellant seeks to rely on observations made by the Grand Chamber in *Big Brother Watch* in relation to RIPA and, in particular, the comments on the need for identification of the categories or types of search terms, the need for prior internal authorisation of strong selectors, or search terms, linked to identifiable individuals and the fact that the certificate issued under section 8(4) of RIPA was expressed in general terms and was insufficiently precise to provide any meaningful restriction (paragraph 387 of the judgment in *Big Brother Watch*). However, the position in relation to the Act is different and, further, Chapter 2 of Part 6 deals with communications data, not interception and examination of content, and the Grand Chamber recognises that the relevant safeguards do not need to be identical in every respect to those applicable to the interception of content. The need to specify the operational purposes, and the need for the Secretary of State, and the Judicial Commissioner to consider that each specified operational purpose is necessary and that the examination of communications data is necessary for those specified operational purposes will act as a constraint upon the examination of such material and does ensure an adequate degree of control over the range of communications data that may be selected for examination. The need for the examination of communications data to be necessary is emphasised again by the Bulk Communications Data Code. There is no provision for prior internal authorisation of strong selectors but the context here is the examination of communications data not content. Furthermore, the duty in section 2, and the provisions of the Bulk Communications Data Code, emphasise the need to consider whether the level of protection to be applied is higher because of the particular sensitivity of the information involved. In all the circumstances, we are satisfied that the totality of the safeguards applicable in relation to the bulk acquisition of communications data is sufficient to guard against the risk of arbitrariness and abuse. They are based in domestic law, are accessible and foreseeable. The interference is therefore in accordance with law for the purposes of Article 8 of the Convention.

Part 6 – Chapter 3

139. Bulk equipment interference warrants authorise the interference with any equipment for the purpose of obtaining communications or equipment data or other information and the selection for examination of material in any manner described in the warrant (section 176).

140. The grounds upon which such a warrant can be obtained are set out in section 178, namely that the warrant is necessary in the interests of national security (or on that ground and for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to national security). The circumstances in which a warrant may be granted appear clearly from section 178 of the Act. A warrant may only be issued if the main purpose is to obtain overseas-related communications, information or equipment data. Decisions must be taken personally by the Secretary of State and the application made by or on behalf of a head of an intelligence service.

141. The process for obtaining such a warrant and the safeguards can be taken together. Paragraph 6.13 of the Equipment Interference Code ("the Equipment

Code") prescribes the material to be included in the application for such a warrant. That will include the background to the application, a description of the equipment to be interfered with and the communications, equipment data and other information to be obtained, a description of the conduct to be authorised, an assessment of the consequences of the conduct, an explanation of why the conduct is considered to be necessary for one of the statutory grounds which must always include an explanation of why it is necessary in the interests of national security, the operational purposes for which communications data may be selected for examination, consideration of whether the material may be made available to overseas authorities, an explanation of why the conduct to be authorised by the warrant is considered proportionate and why it could not be achieved by less obtrusive means and certain assurances. That material will, therefore, be available to the decision-makers.

142. The Secretary of State must be satisfied that the main purpose is to obtain overseas-related communications, information or equipment data and that the warrant is necessary in the interests of national security, either alone or together with one or both of the other two grounds if applicable (section 178). The Secretary of State must consider whether the conduct authorised by the warrant is proportionate to what is sought to be achieved (section 178). That will include consideration of whether what is sought to be achieved could be achieved by less intrusive means (section 2(2)(a)). As the Equipment Code makes clear, that also includes consideration of whether the Secretary of State can foresee the extent of all the interferences to a sufficient degree properly and fully to assess the necessity and proportionality of issuing the warrant. That includes consideration of interferences in relation to all those affected, whether the intended target of the interference or those affected more accidentally. Where that can be considered, usually due to the specific identity of the target being known, or where a specific identifier relating to the target's communications or devices can be used, a bulk equipment warrant is not appropriate (and an equipment interference warrant under Part 5 should be used instead) (paragraph 6.5 of the Equipment Code).

143. The bulk equipment interference warrant that provides for selection for examination must set out the specified operational purposes for which material may be examined and the application will explain why examination is considered necessary for those operational purposes. The need for the warrant to specify the operational purposes for which material may be examined will act as a significant constraint upon the use of search terms. The Secretary of State when issuing the warrant must be satisfied that each of the specified purposes is a purpose for which the examination of material is necessary.

144. Further, the issuing of the warrant is subject to prior independent authorisation by a Judicial Commissioner who must review the necessity for the warrant and whether the conduct authorised by the warrant would be appropriate. In addition, that process includes prior independent authorisation of the specified operational purposes for which intercepted communications and secondary data may be selected for examination. The Judicial Commissioner must consider when deciding whether to approve the decision to issue a warrant that each of the specified operational purposes is necessary *and* that "the examination of

intercepted content and secondary data for each such purpose is necessary" (section 179). The Judicial Commissioner is also required by the Act to have regard to whether what is sought to be achieved "could reasonably be achieved by less intrusive means" (section 2(2)(a) of the Act). The Equipment Code makes it clear that the Judicial Commissioner must consider the necessity and proportionality of the warrant, including whether a targeted equipment interference warrant under Part 5 should be used rather than a bulk equipment interference warrant because the specific identity of the target is known or a specific identifier related to the target individuals' communications or devices can be used (paragraph 6.5 of the Equipment Code). The Judicial Commissioner may also seek further information and clarification and there is an obligation on others to provide such documents as the Judicial Commissioner may need (paragraph 6.29 of the Code and section 235 of the Act).

145. There are further safeguards on the use of the material obtained. Communications cannot be selected for examination of intercepted content by the use of criteria referable to an individual known to be in the British Islands (section 193(4) and the definition of protected material at 193(9)). There are safeguards in relation to the storage and use of material obtained under the warrant (sections 191 and 192). There are further provisions governing copying, storage and destruction in section 9 of the Equipment Code. A warrant lasts for six months (section 184). There are safeguards in relation to the disclosure of material to overseas authorities (section 192 and paragraphs 9.22 to 9.26 of the Equipment Code). There are provisions for oversight and applications to the IPT.

146. The appellant seeks to rely on observations made by the Grand Chamber in *Big Brother Watch* in relation to RIPA and, in particular, the comments on the need for identification of the categories or types of search terms, the need for prior internal authorisation of strong selectors, or search terms, linked to identifiable individuals and the fact that the certificate issued under section 8(4) of RIPA was expressed in general terms and was insufficiently precise to provide any meaningful restriction (paragraph 387 of the judgment in *Big Brother Watch*).

147. The provisions in the Act and the Equipment Code provide a different, strengthened means of ensuring that there are adequate safeguards in relation to bulk equipment interference warrants. There is a need for prior independent authorisation of the warrant. The warrant must specify the operational purposes and the Secretary of State and the Judicial Commissioner must consider whether the examination of material is necessary for those operational purposes. Furthermore, in the context of this statutory regime, we do consider that the fact that the Secretary of State and the Judicial Commissioner will have to consider the nature of the interference authorised by the warrant, and whether less intrusive means (such as a targeted equipment interference warrant) would be sufficient, is significant. That will particularly apply where the specific identity of the target is known, or the warrant relates to a specific identifier related to the targeted individuals' communications devices. The arrangements for authorisation and, importantly, prior independent authorisation, build in a need for consideration of whether the application for a bulk equipment interference warrant is concerned with known specific targeted individuals or their

communication devices and, if so, whether it is appropriate to use a targeted equipment interference warrant instead. That safeguard will, therefore, provide for consideration of whether it would be more appropriate to issue a targeted equipment interference warrant which will be limited to those individuals rather than granting a bulk equipment interference warrant which would permit a wider interference in respect of those who are not the targets of the surveillance but might be affected incidentally. Further, the use of criteria for selecting communications for examination which are referable to an individual within the British Islands is not permitted. The fact that there is a difference in relation to secondary data, which may be examined using criteria referable to an individual within the British Islands does not render the scheme as a whole incompatible. As a general rule, as the Divisional Court observed, at paragraphs 172 to 178 of the Convention Judgment, the examination of content (rather than secondary data) raises greater privacy concerns. Those safeguards ensure a considerable degree of control over the circumstances in which the communications of an identifiable person can be selected for examination.

148. The appellant submits that the safeguards do not provide for the specification of categories or types of search terms or the prior internal authorisation of search terms linked to an identifiable individual and differ from the safeguards applied in relation to bulk interception warrants. We are satisfied that, overall, the safeguards put in place do meet the underlying aims identified in the *Big Brother Watch* judgment in this regard. The safeguards in place, together with the need for prior independent authorisation and the duties on the Judicial Commissioner to consider necessity, proportionality and the question of whether the aims could be achieved by less intrusive means, fulfil essentially the same aim in this context. Furthermore, it is not for this court to determine which arrangements would be preferable and to consider whether the regime used for bulk interception warrants should also be used for bulk equipment interference warrants.

149. The issue for this court is whether viewed in totality, the safeguards governing bulk equipment interference warrants are in accordance with law and contain adequate and effective safeguards against the risk of abuse and arbitrariness. We are satisfied that the safeguards are based in domestic law, and are accessible and foreseeable. We are also satisfied that the safeguards are sufficient. At the very least, given that the position under the Act is very different from RIPA, and given in particular the significantly strengthened safeguards governing Chapter 3 of Part 6 of the Act, we doubt that a domestic court could be fully confident that the absence of particular features referred to in *Big Brother Watch* (notably the absence of a requirement for prior internal authorisation for search terms linked to identifiable individuals) was such a deficiency as to mean that the regime was not in accordance with, or prescribed by, law for the purposes of Articles 8 and 10 of the Convention.

Part 5

150. Part 5 of the Act deals with targeted equipment interference warrants. Such warrants authorise a person to obtain communications, equipment data and other information. The subject matter of such warrants is set out in section 101(1) of the Act. They may relate, essentially, to equipment of a particular

person or organisation, or of a group of persons who share a common purpose or carry on a particular activity, or equipment in one location, or equipment of more than one person or one group or in one location where the interference is for a single investigation or operation. Section 115 of the Act provides that the warrant must include specific details. Where, for example, the warrant relates to equipment belonging to, used by or in the possession of a particular person or organisation, that person or organisation must be named (or a description of the organisation given). Similarly, where the equipment belongs to, or is used by or is in the possession of persons who form a group which shares a common purpose or activity, the warrant must include a description of the activity and the name, or a description of, as many of the persons as it is reasonably practicable to name or describe. Where a warrant relates to equipment where the interference is for a single investigation or operation, the warrant must include a description of the nature of the investigation or operation and the name, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe. Where the equipment is in a particular location, that location must be named in the warrant.

151. The grounds upon which a targeted equipment interference warrant may be sought are set out at section 102 of the Act (and s 106(3) in relation to the purpose of preventing death or injury or damage to a person's mental or physical health). It must be necessary in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as that is relevant to the interests of national security. The circumstances in which a person's equipment may be the subject of such a warrant appears sufficiently from section 101 of the Act as described in the previous paragraph.

152. The Equipment Code prescribes the material which must be included within an application for a targeted equipment interference warrant (paragraph 5.34). That reflects the details that must be included in the warrant by reason of section 115 as discussed above. That information will provide considerable detail about the names of persons or organisations to be the subject of the warrant, or the location of equipment, or the description of the investigation or operation (and a name or description of as many of the persons or organisations as it is reasonably practicable to describe).

153. The Secretary of State must consider that the warrant is necessary for the grounds for which such a warrant is sought and that the conduct authorised is proportionate. The issuing of a warrant is subject to prior approval by a Judicial Commissioner who must be satisfied that the warrant is necessary and that the conduct authorised is proportionate. The Judicial Commissioner will need to comply with the general duties under section 2 of the Act. There are safeguards in relation to storage and disclosure of material (section 129 and paragraphs 9.27 to 9.32 of the Equipment Code). There are safeguards in relation to the disclosure of information to overseas agencies (section 130 and paragraphs 9.22 to 9.26 of the Equipment Code). Warrants last for 6 months. There are provisions for oversight and applications to the IPT.

154. We are satisfied that the regime governing targeted equipment interference warrants is in accordance with law. The regime is based on domestic law, is

accessible and foreseeable. Viewed in totality, the statutory regime provides adequate and effective safeguards against the risk of abuse or arbitrariness. The application for the warrant will provide detailed information about the names and organisations to be subject to the warrant and those details must be included in the warrant itself. There is prior independent authorisation by a Judicial Commissioner of the warrant. The Judicial Commissioner will be provided with the information on the names of persons or organisations, or the details of the single investigation or operation, and can ask for further information or clarification. The Judicial Commissioner will consider if the warrant is necessary for the statutory grounds and also if the conduct authorised is proportionate. The Judicial Commissioner will, therefore, have decided to authorise conduct involving the obtaining of communications, equipment data and other information from named individuals or organisations that are named or described. The examination of material referable to individuals will, therefore, have been the subject of prior independent authorisation. We have no doubt that the safeguards provide adequate and effective guarantee against the risk of abuse or arbitrariness in the use of targeted equipment interference warrants.

155. The appellant relies on the absence of any need to specify categories or types of search terms at the point of authorisation or prior internal authorisation of search terms referable to identifiable individuals, as referred to by the Grand Chamber in *Big Brother Watch*. That submission, however, fails to have regard to the fact that the type of bulk interception powers that the Grand Chamber were dealing with were very different from the kind of targeted equipment interference powers in issue in relation to Part 5 of the Act. Further, the legal regime now in place is very different from that applicable under RIPA. There is prior independent authorisation of the warrant and that involves consideration of the necessity for and proportionality of the warrant. That decision will be taken by the Judicial Commissioner on the basis of the information required to be supplied in the application, and included in the warrant, which includes the names of persons and the names or descriptions of persons to whom the warrant relates. When material is selected for examination, the identity of the persons affected and who will suffer interference will have been considered and approved by the Judicial Commissioner. We do not consider that the description of some of these warrants as thematic assists the legal analysis. We do not see any basis for considering that the regime for Part 5 targeted equipment warrants is deficient.

The Second Issue

Journalistic Communications in relation to Part 3, 4, 5 and 6

156. The submissions on this issue were made by Mr Jaffey and Mr Jude Bunting KC for the Intervener. First it is submitted that the provisions of the amended Chapter 1 of Part 6 did not meet the requirements of *Big Brother Watch*. The provisions which provide for prior independent authorisation of selection of journalistic material did not apply where it was known that selectors were connected to a journalist or where it was likely that confidential journalistic material would be selected for examination, only where that was intended or highly probable, contrary to paragraphs 525 to 528 of *Big Brother Watch*. There

was no express requirement set out in the legislation itself that there be an overriding requirement in the public interest.

157. Secondly, it is submitted that the definitions of journalistic material and confidential journalistic material in the Act would cut back the protections afforded to confidential journalistic material in a way that was incompatible with Articles 8 and 10. The definition of "journalistic material" in section 264(2) was limited to material created or acquired for journalism. The exclusion of material created with the intention of furthering a criminal purpose meant that material that was obtained from a source who provided it to a journalist would not be protected.

158. Thirdly, it is submitted that the Secretary of State was wrong not to accept that the remedial arrangements made for bulk interception warrants in Chapter 1 of Part 6 also need to be applied to Parts 3, 4, 5, and Chapters 2 and 3 of Part 6. Mr Jaffey submits that, if any of these powers could lead to the identification of a journalist's source, it could lead to the consideration of the same material as might be obtained under a bulk interception warrant. The fact that the material was obtained by a different method of surveillance did not justify the absence of such safeguards. Mr Bunting took the Court through a series of European Court, and domestic cases. He submits that the underlying principle in the case law was the Court should concentrate on the effect of what was done. If the effect of the exercise of any of the powers was to result in information being obtained which was likely to disclose a journalist's source, the principles identified by the case law, up to and including the Grand Chamber in *Big Brother Watch*, applied.

159. Sir James Eadie for the respondents submits that on a proper reading of the judgment in *Big Brother Watch* the concern identified by the Grand Chamber was that, in the context of bulk interception warrants, material might be obtained which was known to be connected to a journalist. That would occur if it was intended to obtain such material or it was highly probable that that would be the result. That needed to be the subject of prior independent authorisation.

160. Sir James Eadie submits that the requirement that there be an overriding requirement in the public interest was not a free-standing, separate legal obligation which had to be written into the statutory scheme. Rather that reflects the importance accorded to the protection of journalistic material in the context of press freedom and that has to be considered when assessing whether any interference is necessary and proportionate. Further, the definitions relating to journalistic material do not improperly restrict the protection of journalistic sources or confidential material. Not all material in the possession of a journalist is required to be accorded protection. Material in the possession of a journalist but not acquired for a journalistic purpose does not merit additional protection simply because it might be used at some stage in the future for some journalistic purpose. Similarly, the exclusion of material that is created or acquired for a criminal purpose is not inconsistent with Article 10. Further, properly interpreted, a journalist's source did not lose protection if that source had acquired the information unlawfully.

161. Finally, Sir James submits that the requirements in relation to bulk interception powers could not be applied, or read across, to other types of surveillance powers. Those powers operate in a different way and involve different levels of intrusion. He submits that it may be necessary to have evidence as to how bulk equipment interference warrants operate to assess whether they are comparable to other types of warrants. In relation to the retention and acquisition of data under Parts 3 and 4, or bulk acquisition warrants in Chapter 2 of Part 6, there is nothing in *Big Brother Watch* to suggest that there had to be prior independent authorisation of the acquisition of communications data. The regime governing Part 5 is a different legal regime, with different powers and adequate and effective safeguards. Similarly, the regime in Chapter 3 of Part 6 operates differently from that in relation to bulk interception powers.

Discussion

Part 1 Chapter 6.

162. We are satisfied that the amended section 154 of the Act will satisfy the requirements of Article 10.

163. Sections 154(1) and (2) provide for prior independent authorisation, by the Investigatory Powers Commissioner, where information obtained under a bulk interception warrant is to be selected for examination where:-

> "(a) the purpose, or one of the purposes, of using the criteria to be used for the section of the intercepted content or secondary data for examination ("the relevant criteria") is to identify any confidential journalistic material or to identify or confirm a source of journalistic material or it to identify or confirm a source of journalistic information, or
>
> (b) the use of the relevant criteria is highly likely to identify such material or confirm such a source."

164. Further, section 154(3) as amended will provide that:

> "The Investigatory Powers Commissioner may only give an approval under subsection (2) only if –
>
> "(a) the public interest in obtaining the information that would be obtained by the selection of the intercepted content or secondary data for examination outweighs the public interest in the confidentiality of confidential journalistic material or sources of journalistic material or sources of journalistic information, and
>
> (b) there are no less intrusive means by which the information may reasonably be obtained.

165. Those provisions will ensure compliance with Article 10 of the Convention. Reading *Big Brother Watch* as a whole, the concern in relation to bulk interception warrants was to address circumstances where the intention of the intelligence services is to access confidential material, for example, through the deliberate use of a search term connected to a journalist or where as a result of the choice of search terms, there is a high probability that such material will be selected. In those circumstances, there needed to be prior independent authorisation (paragraph 448). The Grand Chamber went on to apply that approach to the facts of that case, as appears at paragraph 456 to 458 of the judgment. That approach is replicated in the amended section 154 of the Act. The reference in paragraph 525 of the judgment to "likely" must be read fairly and in context. The Grand Chamber was assessing the safeguards in the relevant code of practice governing the acquisition of communications data under RIPA and noted that those provisions "only applied where the purpose of the application for the warrant was to determine a source: they did not apply in every case where there was a request for the communications data of a journalist or where such collateral intrusion was "likely". In paragraph 448, the Grand Chamber was referring to "the deliberate use" of selectors connected to a journalist. The Grand Chamber was not seeking to lay down any general principle, or interpretation of Article 10, which required prior independent authorisation where the request was likely to result in the communications data of a journalist being obtained. It was not seeking to depart from the general approach to this issue described in detail in paragraphs 447 to 450, nor the actual application of that approach to the situation governed by RIPA described at paragraph 456 of the judgment.

166. Similarly, the requirements of the amended section 154(3) make it clear that the Investigatory Powers Commissioner must consider whether the public interest in obtaining the information outweighs the public interest in the confidentiality of journalistic material or sources. That has to be read, of course, in the light of the general duties in section 2(2) which requires a public authority to have regard to whether the level of protection in relation to particular information is higher because of the particular sensitivity of the information, and gives as examples of that material which identifies or confirms a source of journalistic information.

167. The amended section 154 also deals with material where the person considers that obtained material contains confidential journalistic material or material identifying or confirming a journalistic source. The person must notify the Investigatory Powers Commissioner who will order the destruction of the material unless satisfied that the public interest outweighs the interest in confidentiality.

168. Nor are the definitions relating to the protection of journalists such as to reduce inappropriately the protection required. We agree with the Divisional Court that Article 10 of the Convention does not require that any documentation held by a journalist is protected and that the definition in the Act with its reference to material created or acquired for the purposes of journalism is sufficiently broad to ensure the requisite degree of protection under Article 10 (paragraphs 342 to 344 of the Convention judgment). Nor does the exclusion of material created or

acquired for the purpose of furthering a criminal purpose undermine the proper scope of the protection afforded to freedom of the press by Article 10 and, like the Divisional Court, we do not consider that exclusion creates any difficulty with the compatibility of the definition, taken as a whole, with Convention rights (paragraph 352 of the Convention judgment).

169. Finally, we do not consider that that exclusion, contained in section 264(5) of the Act is intended to apply to, or qualify the definition of, a source of journalistic information. Such a source may provide material which he or she has obtained unlawfully to a journalist and the exception would not apply to that material. It is clear from the context of section 264 that it is dealing with material which the journalist has created or acquired with the intention of furthering a criminal purpose. It is not intended to apply to or affect the definition of a source of journalistic information (defined in section 261) who is an individual who acquires information (whether lawfully or unlawfully) and supplies it to a journalist for the purposes of journalism.

170. For completeness, we should say that we do not accept the submission of Mr Bunting that the case law indicates that the sole question is whether any provision has an effect on journalists. It is not necessary, and would be disproportionate, to lengthen this judgment with an analysis of the domestic case law and the Strasbourg case law on which he relied. Those decisions were fully analysed by the Divisional Court and we agree with its analysis. In short, those cases all involved a very different factual context. The questions in this appeal really depend on the application of the decision in *Big Brother Watch* in relation to bulk interception warrants and whether the principles identified in that context can be applied to other types of warrants.

Chapter 2 Part 6

171. Bulk data acquisition warrants under Chapter 2 of Part 6 are concerned with the acquisition of communications data. Such warrants do not authorise the interception and examination of the content of communications. Furthermore, as paragraph 3.1 of the Bulk Communications Data Code recognises, such warrants normally provide for the provision of communications data generated in bulk by a telecommunications operator rather than being targeted at a specific operation. Generally, it is the examination of communications data which might indicate with whom a journalist has been communicating and when, and that, conceivably, may be material that could be used as part of a process of identifying or confirming the identity of a journalist's source. That is likely, if anything, to be the stage in the process which is capable of giving rise to a more significant interference.

172. Paragraphs 6.24 to 6.31 of the Bulk Communications Data Code recognise that issues surrounding the infringement of the right to freedom of expression may arise if communications data is selected for examination for the purpose of identifying the communications data of a journalist, an identified source or where it is done for the purpose of identifying or confirming the identity or role of an individual as a journalist's source. Paragraph 6.25 emphasises the strong public interest in protecting a free press and freedom of expression and where the intention is to select communications data for examination in order to

identify a source of journalistic information "the public interest requiring such selection must override any other public interest". Paragraph 6.28 says that:

> "In the exceptional event that an officer were to select for examination communications data specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand by a person holding the rank of Director of above within their organisation level. Any communications data obtained and retained, other than for the purposes of destruction, as a result of such selection for examination must be reported to the Investigatory Powers Commission at the next inspection."

173. There is also a recognition that even if access to communications data obtained in bulk is not intended to identify a journalist's source, there is a risk that that might occur when examining a journalist's communications data. Paragraphs 6.30 and 6.31 of the Bulk Communications Data Code, therefore, provide that:

> "6.30 The requirement for senior approval does not apply where the intent is to examine communications data obtained in bulk to identify the communications data of a journalist, but it is not intended to determine the source of journalistic information (for example, where the journalist is suspected of involvement in terrorist activity).
>
> 6.31. In such cases there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the officer considers whether the intrusion is justified, giving proper consideration to the public interest. The officer needs to consider whether alternative evidence exists, or whether there are other alternative means for obtaining the information being sought."

174. We are satisfied that the arrangements made for the examination of communications data in the exceptional circumstances where it is to be used to identify or confirm a journalist's identity or source are sufficient to satisfy the requirements of Article 10. They meet the concerns identified by the Grand Chamber in *Big Brother Watch* in relation to the acquisition of communications data (there, under Chapter 2 of RIPA). We are satisfied that the risk of collateral intrusion is safeguarded against by the obligations imposed by section 2(2)(b) of the Act and the provisions of the Bulk Communications Data Code. We are satisfied that the arrangements relating to the protection of confidential journalistic material provide adequate safeguards.

Chapter 3 Part 6

175. Bulk equipment interference warrants may be authorised under Chapter 3 of Part 6. There may be cases, however, where communications have been obtained by means of a bulk equipment interference warrant and the intelligence services wish to examine those communications in circumstances which might reveal a journalist's sources or involve the examination of confidential journalistic information. That is dealt with in paragraphs 9.81 to 9.83 of the Equipment Interference Code. In essence, a senior official must be notified where an authorised person intends to select for examination material obtained under a bulk equipment interference warrant in order to identify or confirm a journalist's source or which is believed to contain confidential journalistic material. The senior officer must approve the selection of the material before the authorised person can examine it and can only do so if satisfied that there are arrangements in place for handling, retaining, using and destroying such material. Where material is not destroyed after examination, that must be reported to the Investigatory Powers Commissioner. There is no requirement, however, that there be prior independent authorisation of the examination of such material.

176. The Grand Chamber in *Big Brother Watch* recognised the importance of the protection of journalists' sources in the context of Article 10 and guaranteeing freedom of expression. The Grand Chamber referred to the need for review by a judge or other independent and impartial decision-making body with a power to determine whether the public interest overrides the principle of protection of journalistic sources prior to the handing over of such material in order to prevent unnecessary access to information capable of disclosing the identity of a journalist's sources (see paragraph 445 of its judgment). Section 2 of the Act also recognises the need to have regard to whether the level of protection is higher because of the particular sensitivity of the information, including information identifying a journalist's source or confidential journalistic material.

177. The question is, therefore, whether the absence of a requirement under Chapter 3 of Part 6 of prior independent authorisation of the use of criteria for examining communications identifying a journalist's source or examining confidential journalistic material is compatible with Article 10. Given the unusual way in which this case has proceeded, we have no judgment from the Divisional Court on this issue. Further, the respondents submit that it may be necessary to have evidence as to how bulk equipment interference warrants operate to assess whether they are comparable to other types of warrant and whether the safeguards identified by the Grand Chamber in relation to the protection of journalists' sources are needed in the context of bulk equipment interference warrants. We bear in mind that we do not have any evidence or information about how equipment interference warrants operate in practice which would enable us to assess these matters. Nor did the Divisional Court have such evidence. In those circumstances, the appropriate course is to remit the question of whether the provisions in Chapter 3 of Part 6 are compatible with Article 10 as they do not include provision for prior independent authorisation of the examination of confidential journalistic material and information capable of

identifying a journalist's sources where that material has been obtained by use of a bulk equipment interference warrant. The respondent can determine whether it wishes to seek to adduce evidence in relation to those matters or whether it wishes to litigate the issue without such evidence.

Parts 3 and 4

178. Parts 3 and 4 of the Act can conveniently be taken together. They concern the giving of a notice requiring retention of communications data and obtaining that data. They are not concerned with obtaining or examining the contents of communications. In the context of protection of confidential journalistic material, a notice given under Part 4 requiring a telecommunications operator to retain communications data is less likely of itself to amount to a significant interference under Article 10 of the Convention.

179. Section 60A of the Act provides that the Investigatory Powers Commissioner may authorise a person to obtain communications data where that is necessary for a specific investigation or a specific operation and the conduct authorised is proportionate. In addition, the Investigatory Powers Commissioner is obliged to have regard to whether there is a need for higher protection in circumstances involving, amongst other things, information confirming a journalist's source (section 2(2)(b) of the Act). Those arrangements provide adequate safeguards to protect journalistic sources when an Investigatory Powers Commissioner authorises the obtaining of data. Section 61 provides for a designated senior officer to grant authorisations for the purpose of a specific investigation or specific operation. Section 77 provides that where such an authorisation is granted in relation to obtaining communications data for the purpose of identifying or confirming a journalist's source, that authorisation cannot take effect until approved by a Judicial Commissioner. The Judicial Commissioner will have to have regard to the public interest in protecting a source of journalistic information and the need for there to be another overriding public interest before a public authority can seek to identify a source of journalistic information (section 77(6)). The Judicial Commissioner is also under the duty imposed by section 2(2)(b) to have regard to the higher level of protection to be applied to sensitive information including information confirming a journalist's source or confidential journalistic information.

180. We are satisfied that those provisions will ensure adequate safeguards against the risk of abuse or arbitrariness. Part 3 deals with the obtaining of communications data not content. The legislative regime taken as a whole does provide adequate safeguards against the risk of abuse or arbitrariness in that context. Authorisations may only be granted where necessary for a specific investigation or a specific operation. The need for prior authorisation by an Investigatory Powers Commissioner, and the specific protection requiring the approval of a Judicial Commissioner when a senior designated official authorises the obtaining of communications data for the purpose of identifying or confirming a journalist's source do provide adequate safeguards in relation to the protection of confidential journalistic material and journalistic sources. The appellant suggests that there may be cases where a senior official grants an authorisation for purposes other than the obtaining information to confirm a journalist's source but where the communications data obtained might reveal

such a source and that situation is not expressly dealt with. We do not consider this to be realistic viewing the legislative regime as a whole. Authorisation is to be granted where necessary for a specific investigation or specific operation and the conduct to be authorised is proportionate. If the investigation or operation involves obtaining communications data to identify or confirm a journalist's source, that is subject to independent authorisation. The regime as a whole is structured to ensure that there are adequate safeguards against the risk of abuse and are in accordance with, and prescribed by, law of the purposes of Articles 8 and 10.

Part 5

181. Targeted equipment interference warrants are related to equipment belonging broadly to, or used by, a particular person or organisation or for a single investigation or operation. In that context, sections 113 and 114 of the Act provide that an application for such a warrant must state if one of the purposes is the obtaining of communications which the applicant believes will contain confidential journalistic material or a source of journalistic material. The Secretary of State may only issue the warrant if, amongst other things, he or she is satisfied that the warrant is necessary and the conduct authorised is proportionate and that there are appropriate safeguards relating to the retention, use and disclosure of such material (sections 102, 113 and 114). The decision to issue a warrant requires prior independent approval by a Judicial Commissioner. We are satisfied that the arrangements relating to the protection of confidential journalistic material and a journalist's source in the context of a targeted equipment interference warrant are adequate and effective to guard against the risk of abuse or arbitrariness and are in accordance with, and prescribed by, law for the purposes of Articles 8 and 10.

182. The appellant submits that there is a deficiency as the safeguards only apply where one of the purposes of the warrant is to determine the source of journalistic information and not to other cases where that may occur. We do not consider this to be realistic, viewing the legislative regime as a whole. A warrant may be granted in relation to a particular person group or organisation or for a single investigation. Where that includes accessing communications believed to contain confidential journalistic material or for identifying or confirming a journalist's source, that must be stated in the application. There will need to be prior independent approval of that as described. The regime as a whole is structured to ensure that there are adequate safeguards against the risk of abuse and are in accordance with, and prescribed by, law of the purposes of Articles 8 and 10.

The Third Issue

Ground 3 and the adequacy of safeguards concerning sharing material overseas in Parts 5 and 6 of the Act

183. Mr Jaffey submits that the arrangements governing the transmission of material to overseas authorities must have certain requirements as set out in paragraph 362 of *Big Brother Watch*. In relation to Parts 5 and 6, however, the relevant provisions of the Act provide that the Secretary of State must make

arrangements to such extent if any as the Secretary of State considers appropriate. That would permit the Secretary of State to reduce the protections to nil as a matter of discretion and that is not in accordance with law for the purposes of Articles 8 and 10 of the Convention.

184. Sir James Eadie submits first that the requirements were identified in *Big Brother Watch* in connection with the transmission of communications obtained by bulk interception to overseas authorities and could not necessarily be applied to transmission of material obtained under other powers. Secondly, the regime under RIPA was held by the Grand Chamber to be compatible with Article 8 as appears from paragraphs 395 to 399 of its judgment. The regime governing transmission overseas of material obtained under the powers conferred by Parts 5 and 6 were either strengthened or materially equivalent to the position under RIPA. In those circumstances, there was no incompatibility with Articles 8 or 10 of the Convention.

Discussion

185. Dealing first with the transmission of material obtained under a bulk interception warrant under Chapter 1 of Part 6, section 151 provides that the Secretary of State "must ensure" that arrangements are in force securing that any material "is handed over to overseas authorities only if" the requirements of subsection (2) are met. That subsection provides so far as material that:

> "(2) The requirements of this subsection are met in the case of a warrant if it appears to the Secretary of State—
>
> (a) that requirements corresponding to the requirements of section 150(2) and (5) and section 152 will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question….."

186. The requirements referred to are those governing disclosure, copying and retention, and examination for specified operational purposes and where necessary and proportionate. Those statutory provisions must be read in the context of the Act as a whole, including section 1(5) which provides that protections for privacy exist by virtue of the Human Rights Act 1998 (which require public authorities to act compatibly with Convention rights).

187. Paragraphs 9.26 to 9.29 of the Interception Code deal with safeguards relating to disclosure of material obtained pursuant to a bulk interception warrant to overseas authorities. Paragraph 9.27 provides that the appropriate issuing authority "must ensure" that material is only handed over to overseas authorities if requirements relating to the minimisation of the extent to which content or secondary data is disclosed, copied, distributed, retained or examined. Paragraphs 9.28 and 9.29 provide that:

> "9.28 As outlined at paragraph 9.27, the Act places a requirement on the issuing authority (the Secretary of State, or where appropriate Scottish Ministers) to ensure that safeguards corresponding to those in the Act should apply, to the extent appropriate, where material obtained under a warrant is being shared with overseas authority. In most circumstances, intelligence sharing will take place with countries with which the United Kingdom has long and established intelligence sharing relationships and which apply corresponding safeguards to material obtained under a warrant as those provided in the Act.
>
> 9.29 But there will also be occasions where material derived from interception warrants may need to be shared with a country overseas with whom we do not have an existing intelligence sharing relationship and whose authorities do not apply safeguards to intercepted material corresponding to those in the Act. Issuing authorities will need to consider the arrangements that should be in place to regulate such disclosure. These should require the person considering the authorising disclosure to balance the risk that material will not be subject to the same level of safeguards that it would be in this country, against the risks to national security if material is not shared."

188. We are satisfied that the arrangements providing for the transmission of material obtained under a bulk interception warrant to overseas authorities are in accordance with or prescribed by law, and contain adequate safeguards against abuse. The statutory framework requires the Secretary of State to ensure that there are arrangements in place relating to disclosure, copying, retention, and examination. The reference to making arrangements to such extent as the Secretary of State considers appropriate has to be read in context. Properly interpreted the power must be used in a way which gives effect to the statutory purpose. The provision is not intended to give the Secretary of State an unfettered discretion as to whether, or what, arrangements are to be made. It is not to be read as giving the Secretary of State power to do whatever he or she thinks appropriate. Rather the purpose of the provision is to require the Secretary of State to ensure that adequate arrangements apply when overseas authorities deal with the material as they do when the material is dealt with by the authorities in the United Kingdom. The requirements must be such as the Secretary of State considers appropriate to achieve that statutory purpose. If there were any doubt about that (which there is not), the Secretary of State is required by section 6 of the HRA, to exercise powers in a way which is compatible with Articles 8 and 10 as recognised by sections 1(5) and 2(4) of the Act. The Secretary of State is, therefore, required by statute to ensure that arrangements are in place which achieve the required protection under the Convention. The Secretary of State could not lawfully consider the

arrangements to be appropriate unless they contained adequate arrangements relating to disclosure, copying, retention and examination such as would apply if the material was being dealt with by the authorities in the United Kingdom.

189. That, again, is reinforced by the provisions of the Interception Code which provides that the issuing authority must ensure that arrangements corresponding to those applicable in the United Kingdom are applied. As paragraph 9.28 recognises, most sharing takes place with overseas authorities with whom the United Kingdom has a long and well-established intelligence sharing relationship and those overseas authorities apply corresponding safeguards. On occasions when that is not the case, the issuing authority will need to consider the arrangements "that should be in place to regulate such disclosure".

190. The arrangements are on any analysis materially similar to those considered to provide adequate safeguards by the Grand Chamber in *Big Brother Watch*. The precautions to be taken when communicating intercept material to overseas authorities are sufficiently clear and afford sufficiently robust guarantees against abuse (see paragraphs 395 to 399).

191. Similar provisions apply in relation to the transmission to overseas authorities of communications data obtained under a bulk acquisition warrant (section 171(9) and paragraphs 9.10 to 9.12 of the Communications Code) and communications obtained under a bulk equipment interference warrant (section 192 and paragraphs 9.33 to 9.35 of the Equipment Interference Code). Similar provisions apply to targeted equipment interference warrants (section 130 and the material parts of the relevant code). We consider, therefore, that the arrangements under Parts 5 and 6 do provide adequate safeguards against abuse and that those safeguards are in accordance with or prescribed by law as they have a basis in domestic law, are accessible and foreseeable.

The Fourth Issue

Ground 5 and Legally Privileged Information and Parts 3, 4, 5 and 6

192. Mr Jaffey submits that the provisions governing access to legally privileged communications, that is, essentially, lawyer-client communications, are insufficient to provide adequate safeguards against abuse. In particular, there is no requirement of prior independent authorisation before selectors or search terms identifying legally privileged information were used. He submits that the need for such a requirement can be seen from the case-law dealing with surveillance. The European Court recognised that Article 8 afforded "strengthened protection to exchanges between lawyers and their clients" (paragraph 118 in *Michaud v France* (2014) 59 EHRR 9). He further relied on observations in *Szabo and Vissy v Hungary* (2016) 63 EHRR 3, particularly at paragraph 77 indicating that prior authorisation was in general required in surveillance regimes. He also relied on observations made in *Kopp v Switzerland* (app No 13/1997/7971000) expressing surprise that the task of determining which communications were legally privileged should be left to an official in the Post Office's legal department.

193. Sir James Eadie submits that the extent of the safeguards required depends upon the degree of interference with respect for a person's private life, relying on *RE v United Kingdom* (2016) 63 EHRR 2. The safeguards in the legislation were adequate and effective and recognised the importance of maintaining the confidentiality of lawyer-client exchanges. The case law does not establish any requirement for independent prior authorisation for examination of privileged material.

Discussion

194. We can deal with this ground of appeal relatively shortly as we consider that the appellant has not demonstrated that the assessment of the Divisional Court at paragraphs 271 to 292 in the Convention judgment is wrong. Further, there is nothing in the judgment of the Grand Chamber in *Big Brother Watch* addressing the question of legally privileged material and no basis for considering that anything said in that judgment undermines the reasoning of the Divisional Court.

195. First, as the Divisional Court observed at paragraph 271, public authorities (which include the issuing authority, the Judicial Commissioner, and the Investigatory Powers Commissioner) must have regard to "whether the level of protection to be applied in relation to any obtaining of information…is higher because of the particular sensitivity of the information" (section 2(2)(b)). Such particularly sensitive information includes "items subject to legal privilege" (section 2(5)(a)). Thus, as the Divisional Court says, "the need to treat such items as sensitive is a principle which suffuses the entire regime in the …Act".

196. Secondly, the Act does have specific protection for legally privileged material. In relation to bulk interception warrants, the significant interference would be the examination of the content of communications containing legally privileged information. Where the purpose of the criteria to be used for selecting intercepted content for examination is to obtain legally privileged material, that must be authorised by a senior official acting on behalf of the Secretary of State. That official must have regard to the public interest in the confidentiality of items subject to legal professional privilege and may only authorise criteria for selecting such material for examination if there are exceptional and compelling circumstances which outweigh the public interest in confidentiality. There are further safeguards if material is examined which is found to contain legally privileged information (whether that was the purpose of the examination or whether that appears on examination of material for other purposes). The Investigatory Powers Commissioner must be notified. He will direct that the item be destroyed unless satisfied that the public interest in retention outweighs the public interest in the confidentiality of material subject to legal privilege, and if retained, may impose conditions on its use (section 153 of the Act). So far as secondary data is concerned, which falls outside content, that last safeguard applies. Similar provisions apply in relation to material obtained pursuant to bulk equipment interference warrants under Chapter 3 of Part 6 (section 194). In addition, the regimes ensure safeguards in relation to storage, copying and disclosure of material as discussed above.

197. We agree with the Divisional Court that those safeguards are adequate and effective guarantees against the risk of abuse in both Chapters 1 and 3 of Part 6. Further, we do not consider that there has to be prior independent authorisation of the use of criteria for examination of such material. None of the case law establishes that as a requirement. In relation to *Szabo,* on which the appellant places particular reliance, that case dealt with secret intelligence gathering powers including covert house searches, recording and opening mail, and recording individuals' electronic communications. It was in that context that the European Court made its general observations in paragraph 77 as to the preferred method of ensuring against the risk of abuse (and even then, did not say that in every case and in every respect, prior independent authorisation was necessary). In relation to *Kopp,* as the Divisional Court noted, that case concerned a situation where the private and professional telephones of a lawyer and his wife were tapped. There had been prior judicial authorisation which stated that "lawyers' conversations were not to be taken into account". It was in that context that the European Court considered the problems with the fact that Swiss law did not state how, under what conditions, and by whom, the distinction between matters connected to a lawyer's work and other matters was to be assessed. The European Court found it astonishing that, in practice, that task should be left to an official in the Post Office legal department. Consequently, the European Court found that Swiss law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion and there had been a violation of Article 8 (paragraphs 73 to 75 of *Kopp*). The decision does not establish that there must be prior independent authorisation of the examination of legally privileged material in all cases.

198. Dealing with communications data under Chapter 2 of Part 6, as the Divisional Court rightly observed a bulk data acquisition warrant does not authorise the acquisition, examination or disclosure of the content of the communication. Whilst the communications data may reveal "when a communication occurred, between which devices and for how long, it will not reveal what was discussed or the subject matter. It will not touch upon the central purpose of legal privilege, namely to enable a client to disclose what he wishes to disclose in order to obtain legal advice, without the fear of the material being disclosed to others without his consent" (paragraph 291 of the Convention Judgment). The same is true of the retention and acquisition of communications data under Parts 3 and 4 of the Act. The general safeguards already discussed in relation to the powers concerning communications data are therefore adequate to ensure that the interference represented by the acquisition and examination of communications data is guarded against.

199. So far as targeted equipment interference warrants under Part 5 are concerned, these operate in a very different way. They are aimed at particular individuals, groups or organisations, or a single investigation or operation. We have described above the range of information that must be provided in an application for such a warrant. In addition, the application must state if one of the purposes of the warrant is to obtain items subject to legal privilege. The person issuing the warrant must have regard to the public interest in confidentiality of items subject to privilege, and only authorise the warrant if there are exceptional and compelling circumstances which make it necessary to authorise the equipment

interference for that purpose. Arrangements must be in place relating to handling, retention, use and destruction of such items (section 112 of the Act). The safeguards are adequate and effective to guard against the risk of abuse.

200. For those reasons, we agree with the Divisional Court conclusion in relation to Parts 3, 4, 5 and 6 (we deal with Part 7 below) at paragraph 292 of its Convention Judgment that:

> "the rules regarding legally privileged items are set out in the … Act and codes of practice with sufficient clarity and sufficient safeguards so as to render the statutory scheme compatible with Article 8."

The Fifth Issue

Part 7 and Grounds 1, 2, 3, 4 and 5

201. The powers conferred by Part 7 are very different in nature and purpose from those provided under the Parts of the Act considered in this judgment. For that reason, it is appropriate to deal with Part 7 separately and to consider the first five grounds of appeal as they apply to the provisions of Part 7.

202. Mr Jaffey submits in relation to ground 4 that the scope of application of Part 7 is so wide and its provisions on retention, use and destruction so discretionary, that it fails to provide the citizen with any indication of what data the state may retain and how it might be used and so does not satisfy the requirement for foreseeability. There is no provision requiring the deletion of data or safeguards relating to disclosure and copying. He relies upon the decision of the Grand Chamber in *Marper v United Kingdom* (2009) 48 EHRR 50, especially at paragraph 99. In relation to Ground 2, he submits that three significant safeguards identified as necessary by the Grand Chamber in *Big Brother Watch* are absent in relation to Part 7 of the Act. In relation to Ground 1, there is no provision governing access to bulk personal datasets in relation to confidential journalistic material or a journalist's source. In relation to Ground 3, there are no safeguards in relation to sharing material with overseas authorities. In relation to Ground 5, the safeguards in relation to legally privileged information are inadequate. Consequently, Mr Jaffey submits that the provisions of Part 7 are not in accordance with law for the purposes of Article 8, are not prescribed by law for the purposes of Article 10 (in relation to confidential journalistic material and a journalist's sources) and did not justify any interference with the rights guaranteed by those Articles.

203. Sir James Eadie submits that the powers conferred by Part 7 are different in kind from bulk interception powers. They do not concern the power to obtain personal data at all, but regulate the way in which the security intelligence agencies dealt with information that they had obtained from a variety of sources and imposed additional safeguards on material that had already been obtained. There are clear, detailed rules and safeguards governing the retention, use and destruction of such information. Bulk personal datasets can only be retained under a warrant and those warrants ceased to have effect at the end of a specified time. In those circumstances, the datasets had to be destroyed as there was no

legal basis for retaining them. There are requirements in the relevant code of practice governing bulk personal datasets which minimised the disclosure and copying of information.

Discussion

204. It is important to consider the regime governing bulk personal datasets in its entirety. First, the provisions in Part 7 do not authorise the interception or obtaining of bulk personal datasets. These are datasets which include personal data relating to a number of individuals most of whom will not be of interest to the intelligence services. The datasets will have been compiled by other persons and obtained by the security services under other powers. The provisions in Part 7 apply when an intelligence service, after an initial examination, decides to retain the set for the purpose of its functions (section 199). Part 7 is therefore intended to control and regulate the use that may be made of bulk personal datasets.

205. Secondly, an intelligence service may not retain or examine a bulk personal dataset unless the retention of the dataset is authorised by a warrant under Part 7 (section 200). There are two kinds of warrant, namely a class bulk personal data warrant and a specific bulk personal data warrant.

206. Thirdly, there are restrictions on what may be retained and examined by means of a class bulk personal data warrant. They cannot be used in relation to protected data. Protected data is data which is not systems data, identifying data or data which is not private information. In essence, therefore class bulk personal data warrants cannot be used for the retention or examination of content (the extent to which secondary material may include content is discussed above). In addition, bulk personal datasets cannot be retained or examined under a class bulk personal data warrant if they include health records or a substantial proportion comprises sensitive personal data (section 202).

207. Fourthly, the more significant interference will therefore occur when the retention or examination of data occurs under a specific bulk personal data warrant. That will enable the retention and examination of a bulk personal dataset where the personal data includes private information about an individual.

208. In summary, the arrangements governing specific bulk personal data warrants are as follows. The application for such a warrant must include a description of the bulk personal dataset and, where authorisation to examine is sought, the operational purpose must be specified (section 205). The Secretary of State must consider the application personally (section 211) and must decide if the warrant is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or the interests of the economic well-being of the United Kingdom so far as relevant to national security. The Secretary of State must also consider that the warrant is proportionate to what is sought to be achieved. He or she must be satisfied that operational purpose itself is necessary and that examination of the bulk personal dataset is necessary for each of the specified purposes (section 205). There are additional safeguards in relation to health records. An application must state if one of the purposes of the warrant

is to authorise the retention and examination of health records or if the head of the intelligence service considers that the bulk personal data dataset includes or is likely to include health records. The Secretary of State may only issue the warrant if there are exceptional and compelling circumstances that make it necessary to authorise the retention and examination of health records. Warrants cease to have effect after 6 months (section 213).

209. There is a requirement for prior approval of a decision to issue a specific bulk personal data warrant (or a class bulk personal data warrant). A Judicial Commissioner must review whether the warrant is necessary for the specified grounds, the conduct authorised is proportionate and whether each specified operational purpose, and examination of data for that operational purpose, is necessary (section 208).

210. There are also additional safeguards if a purpose of the criteria to be used for selecting data for examination is to identify any items subject to legal privilege, or if the criteria are likely to identify such items. If the relevant criteria are referable to an individual known to be in the British Islands, the Secretary of State must approve them and that is subject to approval by the Judicial Commissioner. In other cases, a senior official must approve the use of the criteria (section 222). If such an item is retained after examination, the Investigatory Powers Commissioner must be informed. He must direct that the item be destroyed unless the public interest in retention outweighs the public interest in confidentiality in which case he must impose conditions as to the use or retention of the item (section 223).

211. There are requirements relating to storage and access (paragraphs 7.1 to 7.37 of the Intelligence Services' retention and use of Bulk Personal Datasets Code of Practice ("the BPD Code")). There are provisions dealing with disclosure and copying (paragraphs 7.50 to 7.52 of the BPD Code). There are provisions governing confidential journalistic material and journalists' sources (paragraphs 7.38 to 7.48 of the BPD Code). The approval of a person holding the rank of Director is required where the intention is to select material for examination in order to identify a journalist's source and may only be granted where the public interest in selection overrides any other public interest. Confidential journalistic protected data, and data identifying a journalist's source, should only be retained where it is necessary and proportionate to do so, and must be destroyed when retention is no longer necessary.

212. Furthermore, the Secretary of State, the Judicial Commissioner and the Investigatory Powers Commissioner are subject to the duties imposed under section 2(2) designed to protect privacy, including the need to consider whether what is sought to be achieved could reasonably be achieved by less intrusive measures, and whether the level of protection in relation to obtaining information is higher because of the particular sensitivity of the information. The oversight arrangements in Part 8 of the Act apply and there are rights of appeal.

213. We consider first the case law such as *Marper*. Those authorities deal with the retention and use of data from databases. *Marper* in fact dealt with the retention of DNA and fingerprints. In considering whether the relevant statutory

requirements were in accordance with law for the purpose of Article 8, the European Court observed that there would have to be clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning matters such as duration, storage, use, and preservation of the integrity and confidentiality of the data in issue. It indicated that other contexts, such as telephone tapping, secret surveillance and covert intelligence gathering would need to have such rules. In that case, the European Court did not need to reach a view as to whether the relevant legislation in that case satisfied the quality of law requirement of Article 8(2) of the Convention.

214. We consider that the relevant statutory provisions, and the BPD Code, do provide clear and detailed rules governing the matters relevant to the context here (which does not involve the interception or obtaining of information but the imposition of safeguards on the retention and use of bulk personal datasets compiled by others). The provisions provide clear rules on the need for authorisation for retention and examination of data. There are detailed safeguards provided including, in particular, the need for prior judicial authorisation, which will involve consideration of the necessity for and proportionality of a warrant authorising the retention and examination of datasets. The warrants are limited in duration and it is clear that the data must be destroyed once a warrant expires – the warrant is required for the retention to be authorised and ceases to have effect at the end of a specified time limit. In those circumstances, the data could not lawfully be held and would have to be destroyed. The BPD Code deals with matters such as storage and access.

215. Dealing with the judgment in *Big Brother Watch*, particular care needs to be taken in applying the principles in that case to the situation dealt with in Part 7. *Big Brother Watch* was concerned with bulk interception warrants. Part 7 is not concerned with intercepting communications. Rather it is a set of rules, including safeguards, to regulate the retention and use of datasets compiled by others and obtained by the intelligence services under other powers. In that context, viewed as a whole, the totality of the rules do have a basis in domestic law, they are foreseeable and accessible, and they provide appropriate safeguards.

216. As we have explained, the circumstances in which bulk personal datasets can be retained and examined are set out in the legislation. The process for applying for a warrant, and the procedure for granting it are set out. The application for a specific bulk personal dataset warrant must contain relevant information including the operational purposes for which the material is to be retained and examined. The Secretary of State must be satisfied as to necessity, and the proportionality of the conduct to be authorised. There is, significantly, a need for prior judicial authorisation. The legislation does not refer to the application specifying the types or categories of search terms, and there is no requirement for prior internal authorisation of search terms linked to an identifiable person. However, the need to specify operational purposes, and for the Secretary of State and the Judicial Commissioner to be satisfied that those purposes are necessary and that examination for each of those purposes is necessary, essentially provides a sufficient degree of control over the examination of the bulk personal datasets (bearing in mind that these are datasets already compiled

by others for other purposes and the warrant does not authorise interception of communications or interference with equipment). There are adequate protections for legally privileged information and the protection of journalists' sources. Confidential journalistic material is unlikely to be included in the bulk personal datasets compiled by others but, if and in so far as it is, the Secretary of State and the Judicial Commissioner have a duty to have regard to the need for higher protection for particularly sensitive material. There are provisions in the BPD Code providing further safeguards. Protected data (which is, effectively, the same as the content of communications) cannot be examined under a class bulk personal dataset warrant and requires a specific warrant authorised in the way described above (sections 202 and 203). The protections afforded are materially equivalent to those applicable in other areas where particular types of warrants prohibit the examination of the content of communications of a person within the British Islands. There are oversight arrangements and rights of appeal. Viewed as a whole, those arrangements have a basis in domestic law, they are foreseeable and accessible and provide adequate and effective safeguards against the risk of abuse.

217. The one area that causes us concern is the transfer of data from personal bulk datasets to overseas authorities. Part 7 of the Act itself does not address this issue. There are safeguards elsewhere. Personal data cannot be transferred outside the United Kingdom or to an international organisation unless that is a necessary and proportionate measure carried out for the authority's statutory functions (section 109 of the Data Protection Act 2018). The Grand Chamber in *Big Brother Watch* indicated however, that the transferring state must ensure that the receiving state has safeguards in place for storing data and restricting onwards disclosure although that does not mean the safeguards must be comparable to that in the transferring state (paragraph 362 of the judgment). If the intelligence services transfer data to overseas authorities (something they neither confirm nor deny) they will in fact apply adequate safeguards in practice. These safeguards are set out at paragraph 62 of the judgment of the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [2018] UKIPTrib 15 110 CH (dealing with RIPA but the same arrangements apply it seems to the disclosure of data from bulk personal datasets). Those would ensure that there are adequate arrangements in place to ensure that the transfer of data would not lead to any substantive breach of Article 8. However, the arrangements are not accessible or foreseeable. For that reason and in that respect only, we consider that the failure to make the arrangements publicly accessible would be seen by the European Court as involving a violation of Article 8 of the Convention. We note that there is no prohibition on the transfer of data to overseas authorities. The deficiency identified could be easily remedied in a number of ways, including, for example, amendments to legislation, amendments to the BPD Code, or by making a publicly available statement of the safeguards. We will hear submissions on whether or not any remedy is necessary or appropriate.

218. For those reasons, and subject to this one caveat concerning the transfer of data from bulk personal datasets to overseas, the interference represented by retention and examination of bulk personal datasets is in accordance with law for the purposes of Article 8 of the Convention.

The Sixth Issue

Grounds 6, 7 and 8: The Retained EU Law Grounds

219. Grounds 6 to 8 raise three issues of retained EU law and can be taken together. Mr Jaffey submits that Parts 3, 4, 5 and 6 provide for the general and indiscriminate retention of data within the meaning of retained EU law. Consequently, they require additional safeguards. Further, he submits that the Divisional Court was wrong to find that Part 7 of the Act did not fall within the scope of retained EU law. Some bulk personal datasets are gathered under powers conferred by the Act and directions then given that the provisions of Part 7 apply. To that extent, they fall within retained EU law and involve general and indiscriminate retention of data.

220. In relation to ground 7, Mr Jaffey submits that the Divisional Court was wrong to find, in relation to access to data obtained under Parts 3, 4, 5, 6 and 7, that the requirement for prior approval for access in the context of examining data for purposes other than national security was satisfied by prior independent authorisation at the stage of issuing a warrant. Rather, applying *Watson*, prior independent authorisation is required each time access is sought to examine material.

221. Finally, Mr Jaffey submits that the requirements of Articles 7 and 11 of the Charter provide equivalent protection to equivalent Convention rights. Where the Act is incompatible with the Convention, it will therefore involve a breach of Articles 7 and 11 of the Charter and a remedy could, accordingly, be granted.

222. Sir James Eadie submits first that the Divisional Court was correct to find that none of the relevant powers in the Act are general and indiscriminate in nature within the meaning of EU retained law. Further, the Divisional Court was correct to hold that Part 7 does not fall within the scope of retained EU law. Secondly, Sir James Eadie submits that *Watson* does not require there to be prior independent judicial authorisation each time that data is selected for examination. Finally, Sir James Eadie submits that the Divisional Court was correct to find that the decision of the Grand Chamber is not binding on the CJEU.

Discussion

223. We can consider Grounds 6 and 7 relatively shortly as we see no basis for considering that the Divisional Court was wrong on its central conclusions on these issues.

224. First, as the Divisional Court pointed out, the CJEU in *Watson* was dealing with Swedish legislation which required the general retention of all manner of electronic communications and data for all subscribers and registered users, without differentiation or limitation. The Swedish legislation was not qualified by either a necessity or a proportionality test (paragraphs 121 and 126 of the first EU Judgment).

225. Secondly, the Divisional Court set out at paragraphs 127 to 134 of its first EU Judgment why it considered the provisions of Part 4 of the Act were not general and indiscriminate. We have set those at out paragraphs 82 to 83 above. We consider that that reasoning is correct. The Divisional Court held that the same reasoning applied to Parts 3, 5 and 6 of the Act. We agree. Nor do we consider that that reasoning is affected by anything said by the CJEU in C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*. The regimes in that case are very different to the regimes in the present case. Parts 3, 4, 5 and 6 do not involve the general and indiscriminate retention of data. Rather, the amount of data retained will be the outcome of applying the statutory regime which in turn, involves consideration of questions of necessity and proportionality.

226. So far as Part 7 is concerned, we agree with the Divisional Court that where data is obtained under powers outside the Act, and the safeguards in Part 7 are applied to that data, those situations do not fall within the scope of retained EU law for the reasons given at paragraph 139 of its second EU Judgment set out at paragraph 99 above. There may be an issue as to whether particular bulk datasets acquired under provisions of the Act and made subject by direction to the Part 7 safeguards fall within the scope of retained EU law. But we are satisfied that even if that is the case, the retention of the data would not be general and indiscriminate. The retention of such bulk personal datasets must be authorised by a warrant under Part 7. The application of the Part 7 regime involves the application of tests of necessity and proportionality to determine whether bulk personal datasets can be retained or whether they must be destroyed. Bulk personal datasets are not retained in a general and indiscriminate manner. As none of the regimes involve the general and indiscriminate retention of data, it is not necessary to deal with the other issues raised by the appellant in this regard.

227. In relation to ground 7, the Divisional Court set out at paragraph 145 of the second EU Judgment why it did not consider that *Watson* required prior independent authorisation each time data was accessed and it was sufficient if the initial prior independent authorisation of a warrant authorised access. That paragraph is set out at paragraph 100 above. We agree. Here, retention and access are dealt with at the same time and there is prior independent authorisation of access. There is no requirement under EU law to obtain independent authorisation again. Nothing in the second EU Judgment is inconsistent with that. Nor is that analysis altered by Opinion 1/15 of 26 July 2017 and subsequent CJEU case law. They simply deal with very different factual contexts.

228. Ground 8 essentially concerns remedies. If legislation involves a violation of a Convention right, the only available remedy would be a declaration of incompatibility under section 4 of the HRA. If the legislation also involves a breach of a provision of the Charter, the possibility arises of a remedy directed at disapplying the legislation at least in so far as it breached a provision of the Charter. It is correct that the decision in *Big Brother Watch* would not bind the CJEU. However, there is a different question, which is whether the Charter guarantees equivalent rights.

229. Article 52(3) of the Charter provides that the relevant articles of the Charter are to be given the same effect as the Convention. So far as the matters raised in this appeal in relation to Parts 3, 4, 5 and 6 are concerned, and given that we have considered the legislation as it is proposed to be amended, we have not found any breach of the Convention. There has been no suggestion that the matters complained of in relation to Parts 3, 4, 5 or 6 of the Act would breach any provision of the Charter for any other reason. In the circumstances, Ground 8 does not call for the grant of any remedy in this appeal in relation to those matters.

230. So far as Part 7 is concerned, the only issue that arose under the Convention concerned the publication of adequate safeguards in relation to the transfer of data from bulk personal datasets to overseas authorities (see above paragraph 202). However, where data is obtained under powers outside the Act, this would not fall within the scope of EU law. The appellant said in argument that on a small number of previous occasions, bulk personal datasets were obtained under the Act and then a direction given under section 225 of the Act that Part 7 applied. These judicial review proceedings, and this appeal, were not intended to review particular transfers that have occurred in the past. We were not shown any evidence or any directions dealing with these instances. It is, therefore, neither necessary nor appropriate, to consider any remedy in relation to past events that may have happened. In relation to the future, the United Kingdom has ceased to be a member of the European Union and the provisions of the Charter would not be applicable to any future transfers as it is not part of any retained EU law. No remedy is needed therefore, so far as the Charter is concerned, in relation to Part 7 of the Act.

Conclusion

231. We have set out our conclusions at paragraph 12 above. This appeal will be dismissed for the reasons set out above, subject to two matters. First, the arrangements governing the transfer of material from bulk personal datasets to authorities in other states are not in accordance with law, and so not compatible with Article 8 of the Convention, because the safeguards governing such transfers are not contained in any legislation, code or publicly available policy or other document. We will invite written submissions on the appropriate remedy on this matter. Secondly, we will remit the following issue to the Divisional Court for its determination: whether the provisions of Chapter 3 of Part 6 are sufficient to provide adequate safeguards for the protection of a journalist's sources or confidential journalistic material in relation to communications obtained by means of a bulk equipment interference warrant.

ANNEX:

OVERVIEW OF RELEVANT LEGISLATION

[This document has been agreed between the parties, subject to three "riders" by the Claimant, which are set out below where relevant]

Contents

1. This document presents an overview of the regime introduced by the Investigatory Powers Act 2016 (the "**Act**" or, where clarity requires, the "**2016 Act**"), and certain other relevant legislative provisions. It is intended to be an introduction to the structure and operation of the legislation. It does not refer to all of the relevant provisions for the purposes of the claim.

I) GENERAL PRIVACY PROTECTIONS – PART 1 OF THE ACT

2. The Act sets out "*the extent to which certain investigatory powers may be used to interfere with privacy*": s.1(1).

3. Part 1 of the Act contains both general "*duties in relation to privacy*" and other protections including offences and penalties: s.1(2)-(3).

4. S.2 of the Act contains "general duties" in relation to privacy in s 2(2). The duties apply where a public authority[1] is deciding whether to issue, renew or cancel a warrant under Parts 2, 5, 6 or 7 (as the Secretary of State may do: see below), to approve such a decision (as a Judicial Commissioner may do: see below), to grant, approve or cancel an authorisation under Part 3, or to give a notice under Part 4: s.2(1).

5. In exercising the specified functions, s.2(2) provides that 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 [2],*
> *(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*".

6. The 'have regard' duties in s.2(2) apply so far as is relevant in the particular context, and subject to the need to have regard to other considerations that are also relevant in that context: s.2(3). Section 2(4) provides that those other considerations may 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.*"

7. Part 1 of the Act also contains certain criminal offences, namely, intentional "unlawful interception" (s.3) and knowingly or recklessly "unlawfully obtaining communications data" (s.11).

8. *Unlawful interception* occurs where (a) a person intentionally intercepts[3] a communication in the course of its transmission by a public or private telecommunications system or a public postal service, (b) the interception is carried out in the UK and (c) the person lacks "*lawful authority*" to do so: s.3(1). So far as is material to the present claim, lawful authority will exist (inter alia) where the interception is carried out in accordance with a bulk interception warrant under Pt 6, Ch 1 of the Act: s.6(1)(a)(ii). The offence of unlawful interception is

[1] Defined as "*a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal*": s.263(1).
[2] Section 2(5) gives certain examples of sensitive information for these purposes, including "*items subject to legal privilege*" and "*any information identifying or confirming a source of journalistic information*".
[3] Interception (etc.) for these purposes is defined in s.4 of the Act. In summary, it consists of doing a 'relevant act' in relation to a system (namely modifying or interfering with the system or its operation, monitoring transmissions made by means of the system, or monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system), whose effect is to make the content of any communication available to a person who is not the sender or intended recipient of the communication.

triable 'either way', and, on conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.3(6). Section 7 of the Act makes provision for the imposition of monetary penalties (of up to £50,000) by the Investigatory Powers Commissioner in cases of interception without lawful authority which do not, in the Commissioner's view, amount to the offence of unlawful interception, but this provision does not apply where a person was "*making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception*".

9. *Unlawfully obtaining communications data* occurs where, without lawful authority[4], a relevant person[5] knowingly or recklessly obtains communications data from a telecommunications operator or postal operator: s.11(1). It is a defence if the person can show that s/he acted in the reasonable belief that s/he had lawful authority to obtain the communications data. The offence of unlawfully obtaining communications data is also triable 'either way', and, on conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.11(4)(d).

II) BULK INTERCEPTION, ACQUISITION AND EQUIPMENT INTERFERNCE WARRANTS – PART 6

10. This claim concerns, inter alia, the 'bulk warrant' provisions in Part 6. In that regard:
    a. Pt 6 Ch 1 provides for bulk interception warrants.
    b. Pt 6 Ch 2 provides for bulk acquisition warrants (for communications data).
    c. Pt 6 Ch 3 provides for bulk equipment interference warrants.

11. The key provisions are set out below (bulk personal datasets, under Pt 7 of the Act, are considered separately).

(a) Bulk interception warrants (Pt 6 Ch 1)

12. A bulk interception must satisfy the following two cumulative conditions:

    a. Its "*main purpose*" is either the interception of "*overseas-related*" communications (i.e. communications sent or received by individuals who are outside the British Islands) or the obtaining of "*secondary data*" from such communications (s.136(2)); and

    b. The warrant authorises or requires its addressee to secure, by any conduct described in the warrant, one or more of (a) the interception, in the course of their transmission by means of a telecommunication system, of "*communications*" described in the warrant; (b) the obtaining of "*secondary data*" from such communications; (c) the "*selection for examination*", in any manner described in the warrant, of "*intercepted content*" or "*secondary data*" obtained under the warrant; or (d) the "*disclosure*", in any manner described in the warrant, of anything obtained under the warrant to its addressee or any person acting on their behalf (s.136(4)).

[4] S.81 makes provision for the circumstances in which conduct authorised by Pt 3 ('*Authorisations for obtaining communications data*') will be considered to be lawful.
[5] Defined in s.11(2) as a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

13. A bulk interception warrant also authorises any conduct which it is necessary to undertake in order to do what is expressly authorised or required (s.136(5)).

14. "*Communication*" by s 261(1) relevantly includes "*anything comprising speech, music, sounds, visual images of data of any description*" and "*signals serving either for the impartation of anything*" between persons or things (or both) "*or for the actuation or control of any apparatus*". A communication may therefore be or contain "*content*" and/or "*secondary data*" (see immediately below).

15. "*Content*" by s 261(6) means relevantly "*any element of* [a] *communication, or any data attached to or logically associated with* [a] *communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but — (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and (b) anything which is systems data is not content.*" (By s 157(1), "*intercepted content*" in relation to a bulk interception warrant means "*any content of communications intercepted by an interception authorised or required by the warrant*".)

16. "*Secondary data*" by s 137 means either of the following:

    a. First, "*systems data*" which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise) (s 137(4)). "*Systems data*" means "*any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of*" a postal service, a telecommunications system (including any apparatus that forms part of it), any telecommunications service provided by means of a telecommunication system, any system on which communications or other information are held (including any apparatus forming part of it) (a "*relevant system*"), and any service provided by means of a relevant system (s.263(4)– (5)).

    b. Secondly, "*identifying data*" that—(a) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise), (b) is capable of being logically separated from the remainder of the communication, and (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication (s.137(5)). "*Identifying data*" means data which may be used to identify, or assist in identifying, any person, apparatus, system, service, event or the location of any person, event or thing (s.263(2)–(3)).

(b) Bulk acquisition warrants (Pt 6 Ch 2)

17. Bulk acquisition warrants authorise the obtaining, imposition of a requirement to obtain, "*selection for examination*" and disclosure of "*communications data*".

18. Specifically, a bulk acquisition warrant authorises or requires its addressee to secure, by any conduct described in the warrant, any one or more of (see s.158(5) and (6)):

    a. requiring a telecommunications operator specified in the warrant (i) to disclose to a person specified in the warrant any "*communications data*" which is specified in the warrant and is in the possession of the operator, (ii) to obtain any communications data specified in the warrant which is not in the operator's possession but which the operator is capable of obtaining, or (iii) to disclose to a person specified in the warrant any data so obtained;

    b. the selection for examination, in any manner described in the warrant, of communications data obtained under the warrant;

    c. the disclosure, in any manner described in the warrant, of communications data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

19. "*Communications data*" ("**CD**") is defined in s.261(5), as follows:

> "*'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 does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.*"

20. Bulk acquisition warrants again authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant (s.158(7)).

(c) Bulk equipment interference warrants (Pt 6 Ch 3)

21. A bulk equipment interference warrant (s.176(1)):

    a. authorises or requires its addressee to "*secure interference with any equipment*" for the purpose of obtaining "*communication*", "*equipment data*" or "*any other information*"; and

    b. has as its "*main purpose*" to obtain "*overseas-related*" communications, information or equipment data.

22. In Pt 6 Ch 3:

    a. "*Communication*" again includes (a) anything comprising speech, music, sounds, visual images or data of any description and (b) signals serving either for the impartation of anything between persons or things (or both) or for the actuation or control of any apparatus (s.198(1)).

    b. "*Equipment*" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment (s.198(1)).

    c. "*Equipment data*" means either:

        i. "*Systems data*" (as defined in paragraph 16 above); or

        ii. "*Identifying data*" (as defined in paragraph 16 above) that is comprised in, part of, attached to or logically associated with, and is capable of being logically separated from, a communication or any other item of information without revealing anything of what might reasonably be considered to be the meaning of that communication / item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact (s.177(1)(b), (2)).

    d. "*Overseas-related information*" means information of individuals who are outside the British Islands (s.176(2)).

    e. "*Overseas-related communications*" are communications sent or received by individuals outside the British Islands (s.176(2)).

    f. "*Overseas-related equipment data*" means "*equipment data*" which (a) forms part of, or is connected with, overseas-related communications or overseas-related information, (b) would or may assist in establishing the existence of overseas-related communications or overseas-related information or in obtaining such communications or information, or (c) it would or may assist in developing capabilities in relation to obtaining overseas-related communications or overseas-related information (s.176(3)).

23. A bulk equipment interference warrant (s.176(4)):

a. must authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates; and

b. may also authorise or require the person to whom it is addressed to secure:

i. the selection for examination, in any manner described in the warrant, of any material so obtained; and/or

ii. the disclosure, in any manner described in the warrant, of any such material to the addressee or any person acting on their behalf.

24. Again, bulk equipment interference warrants authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant: s.176(5).

(d) Criteria for approval of bulk intercept, acquisition and equipment interference warrants by the Secretary of State

25. In the case of all three types of bulk warrant in Part 6, the power to issue a warrant resides with the Secretary of State, and is exercisable only following an application made by or on behalf of the head of an intelligence service (s.138(1), s.158(1) and s.178(1)).

26. In each case, the Secretary of State may only issue the warrant if s/he considers that:

a. the warrant is necessary in the interests of national security[6] or on that ground and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security[7]; and

b. the conduct authorised by the warrant is proportionate[8] to what is sought to be achieved by that conduct[9];

c. each of the specified "*operational purposes*" (see below) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and the examination of material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary[10];

[6] s.138(1)(b)(i), s.158(1)(a)(i), s.178(1)(b)(i).
[7] s.138(1)(b)(ii) and (2), s.158(1)(a)(ii) and (2), s.178(1)(b)(ii) and (2). A warrant may be considered necessary on the "economic well-being" ground only if the information / communications data which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands (s.138(3), s.158(3)) or if the interference with equipment which would be authorised by the warrant is considered necessary for the purposes of obtaining information relating to the acts or intentions of persons outside the British Island (s178(3)).
[8] The requirements of necessity and proportionality are addressed in Interception CoP, §§6.22-6.26; Bulk Acquisition CoP, §§4.6-4.11; Bulk EI CoP, §§6.15-6.19.
[9] s.138(1)(c), s.158(1)(b), s.178(1)(c).
[10] s.138(1)(d), s.158(1)(c), s.178(1)(d)

d. satisfactory arrangements made for the purposes of safeguards relating to disclosure etc. (see below) are in force in relation to the warrant[11];

e. the decision to issue the warrant has been approved by a Judicial Commissioner[12]. However, in relation to bulk equipment interference only, the requirement for prospective Judicial Commissioner approval does not apply where the Secretary of State considers that there is an urgent need to issue the warrant (see below for the provisions that require retrospective Judicial Commissioner approval in such cases).

27. In the case of bulk interception warrants and bulk equipment interference warrants only, the Secretary of State must additionally consider that:

a. in the case of bulk interception warrants, the main purpose of the warrant is the interception of overseas-related communications and/or the obtaining of secondary data from such communications (s138(1)(a)); and

b. in the case of bulk equipment interference warrants, the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data (s.178(1)(a)).

28. Detailed provision as to the format of, and the matters that must be included in, warrant applications under Part 6 Chs 1-3 of the Act appears at: §§6.17-6.20 of the Interception of Communications Code of Practice (the "**Interception CoP**") (bulk interception warrants); §§4.1-4.5 of the Bulk Acquisition of Communications Data Code of Practice (the "**Bulk Acquisition CoP**") (bulk acquisition warrants); and §§6.10-6.13 of the Equipment Interference CoP (the "**EI CoP**") (bulk equipment interference warrants).

29. In relation to all three types of bulk warrant, the decision to issue a warrant must be taken personally by the Secretary of State, and the warrant must be signed by the Secretary of State (s.141, s.160, s.182)[13].

30. Each of the three forms of bulk warrant under Pt 6 Chs 1-3 must, as issued, contain a provision stating that it is a bulk warrant of that kind and it must be addressed to the head of the intelligence service by whom or on whose behalf the warrant application was made; and it must describe the conduct that is authorised by the warrant (s.142(1)- (2), s.161(1)-(2), s.183(1)-(2)[14]). It must also specify the operational purposes for which any material obtained under the warrant may be selected for examination: see under "Operational Purposes" below.

(e) Necessity and proportionality

31. Warrants under Pts 6 Ch 1-3 of the Act may only be issued where the Secretary of State considers a warrant to be necessary for the specified statutory purposes (i.e. national security,

[11] s.138(1)(e), s.158(1)(d), s.178(1)(e)
[12] s.138(1)(g), s.158(1)(e), s.178(1)(f).
[13] Bulk equipment interference warrants may be signed by a designated senior official if it is not reasonably practicable for the warrant to be signed by the Secretary of State: ss.182(3)–(4) and EI CoP §§6.21-6.22.
[14] In the case of a bulk equipment interference warrant, the warrant must also "*describe the conduct that is authorised by the warrant*" (s.183(3)).

or national security *together with* the prevention /detection of serious crime or the interests of the economic well-being of the UK (so far as also relevant to the interests of national security), and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means (see s.2(2)(a) of the Act, as referred to above).

(f) Operational purposes

32. The Secretary of State may not issue a bulk warrant under Pt 6 Ch 1, 2 or 3 unless s/he considers that (i) each of the "*specified operational purposes*" is a purpose for which the examination of material obtained under the warrant is or may be necessary, and (ii) the examination of material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary: s.138(1)(d), s.158(1)(c), s.178(1)(d).

33. In that regard, a bulk warrant under each of Pt 6 Chs 1-3 must "*specify the operational purposes for which any [material] obtained under the warrant may be selected for examination*" (s.142(3), s.161(3), s.183(4)).

34. By ss.142(4)-(11), 161(4)-(11) and 183(5)-(12):

a. The operational purposes specified in a warrant must be in a "*list of operational purposes*" maintained by the heads of the intelligence services as purposes which they consider are operational purposes for which material obtained under the type of bulk warrant may be selected for examination.

b. An operational purpose may be specified in that list only with the approval of the Secretary of State, who may give such approval only if satisfied that the operational purpose is "*specified in a greater level of detail than*" "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom so far as … relevant to the interest of national security*".

c. The list of operational purposes must be provided by the Secretary of State to the Intelligence and Security Committee of Parliament every three months. The Prime Minister must review the list of operational purposes at least once a year.

d. A warrant may specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

e. The Codes of Practice indicate that the practice will (other than in exceptional circumstances) always be that *all* operational purposes (for the type of warrant) are included in every warrant: Interception CoP §6.67-6.68; Bulk Acquisition CoP §6.10; EI CoP §§6.6-6.7.

35. Interception CoP §§6.61-6.67 makes further provision relating to operational purposes.[15]

(g) Existence of safeguards

[15] And see Bulk Acquisition CoP §6.3 *et seq*, EI CoP §6.67 *et seq*.

36. Warrants in respect of the bulk powers in Pt 6 Chs 1–3 may only be issued if the Secretary of State considers that satisfactory "*safeguards*" are in place in respect of a number of matters: s.138(1)(e), s.158(1)(d), s.178(1)(e). Again, the relevant safeguards are largely the same in relation to each of the three key bulk powers.

(i) Safeguards relating to retention, copying and disclosure

37. In relation to every bulk (Pt 6) warrant, the Secretary of State must ensure that arrangements are in force for securing that:

    a. In relation to material obtained under the warrant, each of the following is limited to the minimum that is necessary for the "*authorised purposes*":

        i. the number of persons to whom any of the material is disclosed or otherwise made available;

        ii. the extent to which any of the material is disclosed or otherwise made available;

        iii. the extent to which any of the material is copied; and

        iv. the number of copies that are made;[16] and

    b. every "*copy*" made of any "*material*" obtained under a warrant is destroyed as soon as there are no longer any "*relevant grounds*" for retaining it[17];

    and

    c. specific safeguards relating to the examination of material are also in place[18] (see "Safeguards relating to selection for examination" below).

38. As to (a), the meaning of "*necessary for the authorised purposes*" is elucidated in the same terms for each of the three bulk powers: see s.150(3), s.171(3) and s.191(3)[19].

---

[16] See s.150(1)(a) and (2); s.171(1)(a) and (2); and s.191(1)(a) and (2).

[17] See s.150(1)(a) and (5); s.171(1)(a) and (5); and s.191(1)(a) and (5). There will no longer be any relevant grounds for retaining a copy of any material if, and only if, "*(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or [national security together with one of the other specified grounds], and (b) its retention is not necessary for any of the purposes mentioned [in s.150(3)(b)-(e), s.171(3)(b)-(e) or s.191(3)(b)-(e) as the case may be]*": see s.150(1)(6), s.171(1)(6), s.191(1)(6). "Copy" has a statutory definition: see s.53(10) in relation to interception, s.191(9) in relation to material obtained under a bulk EI warrant, s.171(10) in relation to material obtained under a Bulk Acquisition warrant.

[18] See s.150(1)(b); s.171(1)(b); and s.191(1)(b)

[19] Specifically, "*something is necessary for the authorised purposes if, and only if—*

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 138(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923."

The arrangements for ensuring that the requirements in s.150(2), s.171(2) and s.191(2) are met (i.e. that the various specified matters are kept to the minimum necessary for the authorised purpose) must include "*arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner*": s.150(4), s.171(4) and s.191(4).

39. However, where material obtained under a warrant (or a copy) has been provided to any overseas authority, these safeguards do not apply: s.150(8), s.171(8) and s.191(8). Instead, the Secretary of State must ensure that requirements corresponding to those immediately above and immediately below apply "*to such extent (if any) as the Secretary of State considers appropriate*": see s.151(1) and (2)(a), s.171(9) and s.192(1)-(2).[20]

40. Pt 6 Ch 1 and Pt 6 Ch 3 contain statutory duties not to make "*unauthorised disclosures*" (s.156 and s.197), including disclosure of any material obtained under bulk interception or bulk equipment interference warrants, save where the disclosure is an "*excepted disclosure*" (including a disclosure authorised by the warrant, a disclosure to oversight bodies, etc.). It is a criminal offence to make an "*unauthorised disclosure*" of this kind[21]. Under Pt 6 Ch 2, s.174 makes it an offence for the telecommunications operator required to assist with the warrant (or a person employed or engaged for its business) to disclose the existence or contents of the warrant itself, but there is no offence of disclosing what is collected under a bulk acquisition warrant.

41. Each relevant CoP contains provisions addressing retention, copying and disclosure: Interception CoP §§9.15-9.31; Bulk Acquisition CoP §§9.4-9.13; EI CoP §§9.1-9.35.

(ii) Safeguards relating to selection for examination

42. The Act also requires the Secretary of State to ensure that safeguards relating to the examination of material are in force before issuing a bulk interception warrant, a bulk acquisition warrant or a bulk equipment interference warrant (ss.150(1)(b) and 152; ss.171(1)(b) and 172; and ss.191(1)(b) and 193)). Specifically, s/he must ensure that:

    a. The "*selection for examination*" of any material obtained under a warrant is carried out only in so far as is "*necessary for the operational purposes specified in the warrant*" at the time of the selection for examination (ss.152(1)(a), (2), 172(1)(a), (2)-(3) and 193(1)(a), (2)); and

[20] In the case of bulk interception warrants, the Secretary of State must additionally ensure that restrictions are in force which would "*prevent, to such extent (if any) as the Secretary of State considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in a prohibited disclosure*": s.151(1) and (2)(b). Under s.151(3), "*prohibited disclosure*" means a disclosure which, if made in the United Kingdom, would breach the prohibition in s.56(1) of the Act, which provides that no evidence may be adduced (etc.) in legal proceedings which either discloses, in circumstances from which its origin in 'interception-related' conduct may be inferred, any content of an interception communication or any secondary data obtained therefrom, or which tends to suggest that any interception-related conduct has or may have occurred or is going to occur. (Interception-related conduct is defined in s.56(2) and, read with s.156(1), covers matters such as the making of an application by any person for a warrant, or the issue of warrant, under Pt 6 Ch 1.) The prohibition in s.56(1) is subject to various exceptions set out in Schedule 3.

[21] See: ss.57-59 and 156 (bulk interception warrants); ss.132-134 and 197 (bulk interception warrants).

b. The selection of any of such material is "*necessary and proportionate in all the circumstances*" (ss.152(1)(b), 172(1)(b), 193(1)(b)).

43. Because an operational purpose may be included in a warrant for any of the purposes for which a warrant is issued, "*selection for examination*" may occur for "*operational purposes*" considered necessary for any of "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom*" insofar as relevant to national security.

44. In relation to bulk interception warrants and bulk equipment interference warrants, the Secretary of State must also ensure that the selection for examination of respectively "*content*" and "*protected material*" meets any of the "*selection conditions*" (s.152(1)(c) and s.193(1)(c)) (the "**British Islands safeguard**".) The selection conditions are as follows (s.152(3) and s.193(3)):

a. Selection of the material for examination does not breach the prohibition on the use of selection criteria that are (i) referable to an individual known to be in the British Islands at that time and (ii) used for the purpose of identifying (a) the content of communications sent by or intended for that individual (for a bulk interception warrant) or (b) "*protected material*"[22] consisting of communications sent by, or intended for, that individual or "*private information*" relating to that individual (for bulk equipment interference warrants): ss.152(3)(a) and (4), 193(3)(a) and (4). Sections 152(4) and 193(4) respectively prohibit such selection for examination.

b. The warrant addressee "*considers*" (for a bulk interception warrant) or "*reasonably considers*" (for a bulk equipment interference warrant) that the selection for examination does breach that prohibition: ss.152(3)(b) and 193(3)(b));

c. The selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by, respectively, s.152(5) or s.193(5), which authorise selection for examination where someone enters the British Islands or it becomes apparent that a belief that they were not in the British Islands was mistaken and a "*senior officer*" authorises continued selection for examination for up to five working days[23]; or

[22] Meaning any material obtained under the warrant other than material which is equipment data (see definition at §22.c above) or information (other than a communication or equipment data) which is not private information: s.193(9).

[23] These dis-apply the prohibition on selection for examination of material referable to a person known to be in the British Islands for the purpose of identifying their communications or where (a) criteria referable to an individual have been, or are being, used for the selection for examination of "*content*" / "*protected material*" in circumstances where the prohibition was not breached (or the addressee of the warrant considers it would not be breached, in the case of a bulk interception warrant, or reasonably considers it would not be breached, in the case of a bulk equipment interference warrant), (b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual which would mean that the selection of the relevant content for examination would breach the prohibition, (c) since that time, a written authorisation to examine the relevant content using those criteria has been given by a senior officer, and (d) the selection of the relevant content for examination is made before the end of the "permitted period", being the fifth working day after the time at which the relevant change in circumstances appears to the addressee of the warrant: ss.152(5)(d) and (7); 193(5)(d) and (7)). "*Relevant change of circumstances*" means either that the individual concerned has entered the British Islands or that the addressee of the warrant was mistaken in believing that the individual was outside the British Islands: ss.152(6), 193(6).

d. Selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by a targeted examination warrant issued under either Ch 1 Pt 2 or Pt 5.

Claimant's "rider":

(1) The British Islands safeguard in s 193(1)(c) for bulk interception warrants and bulk equipment interference warrants applies only to "*selection for examination*" of "*content*" (s 152(1)(c)) and "*protected material*" (s 193(1)(c)) respectively and not to other material obtained under a warrant. This is a central feature of this safeguard.

(2) There is no British Islands safeguard for bulk acquisition warrants under Pt 6 Ch 2.

45. The relevant Codes of Practice make further provision in relation to selection for examination: Interception CoP §6.71 *et seq*, Bulk Acquisition CoP §6.14 *et seq*; EI CoP §6.66 *et seq*.

(iii) Enhanced safeguards – special cases

Legally privileged material: bulk interception and bulk EI

46. **Basic position:** As to legally privileged material, the basic position for bulk interception and bulk equipment interference warrants is that:

a. Where "*intercepted content*" / "*protected information*" is selected for examination using criteria the (or a) purpose of which is, or use of which is likely, to identify legally privileged items, a senior official acting on behalf of the Secretary of State must approve the use of such criteria, having regard to "*the public interest in the confidentiality of the items subject to legal privilege*": ss.153(1)-(2),194(1)-(2).

b. Approval may be given only if the official considers that there are specific arrangements in place for the handling, retention, use and destruction of items subject to legal privilege: ss. 153(4)(a), 194(4)(a).

c. In addition, where the (or a) purpose of using the criteria is to identify legally privileged items (but not otherwise, in particular not where the use of such criteria is likely to identify privileged items), approval may be given only if there are "*exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria*": ss.153(4), 194(4). An exhaustive definition of exceptional and compelling circumstances is set out in the Act (ss.153(5) and 194(5)).

47. **Communications furthering a criminal purpose:** Where the (or a) purpose of the use of criteria for selection for examination of "*intercepted content*" / "*protected information*" (but not other material obtained under a warrant) is to identify communications / information that would be subject to legal privilege if they were not made / created or held with the intention of furthering a criminal purpose, one of the "selection conditions" is met (see above) and the warrant addressee considers that the items are "*likely to be communications made with the intention of furthering a criminal purpose*", the selection for examination may occur only if a "*senior official*" has approved the criteria: ss.153(6)-(7), 194(6)-(7). Approval may be given only if the official "*considers*" that the items "*are likely to be*" made / held or created "*with the intention of furthering a criminal purpose*": ss.153(8), 194(8).

48. **Where targeted examination warrants are required and the purpose is to select privileged items:** Where a targeted examination warrant is required in order to select for examination items subject to legal privilege[24] and the (or a) purpose is to authorise the selection for examination of items subject to legal privilege, s.27 and s.112 provide that: the warrant application must state that purpose; the person determining the application must have regard to the public interest in the confidentiality of items subject to legal privilege; and the person determining the application must issue a warrant only if s/he considers that (i) there are exceptional and compelling circumstances that make it necessary to select such items for examination and (ii) the relevant safeguards include specific arrangements for the handling, use, retention and destruction of such data (s.27(2)-(4), s.112(2)-(4)). The same definition of exceptional and compelling circumstances is used in s.27(6) and s.112(6).

49. **Retention following selection for examination:** Where an item subject to legal privilege is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the Investigatory Powers Commissioner ("**IPC**") as soon as is reasonably practicable. The IPC must, unless he considers that the public interest in retaining the item outweighs the public interest in its confidentiality, and that retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury, direct that the item is destroyed or impose conditions as to the use/retention of the item: ss.153(9)-(12), 194(9)-(12).

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that empower the IPC to give directions in relation to legally privileged material (ss 153(9)–(12) and 194(9)–(12)) do not prohibit the use of dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

50. **Definition of "legal privilege":** "Items subject to legal privilege", in relation to England and Wales, has the same meaning as in s.10 Police and Criminal Evidence Act 1984; other definitions apply to Scotland and Northern Ireland: see s.263.

51. **CoP provision:** The safeguards applicable to the selection for examination of legally privileged material are explained at §9.48 *et seq* of the Interception CoP and §9.55 of the EI CoP. Among other matters, pursuant to the Interception CoP and Bulk EI CoP:

    a. Where an application for a targeted examination warrant is made where the (or a) purpose is to obtain items that would be subject to legal privilege, if they were not made with the intention of furthering a criminal purpose, the application must contain a statement to that effect and the reasons for believing that the criminal purpose exception applies: Interception CoP §9.57; Bulk EI CoP §9.53.

    b. Wherever a person to whom a targeted examination warrant relates is a lawyer known to be acting in a professional capacity, or where communications are to be selected for examination using criteria referable to such a person, the authority must assume that the statutory protections for legally privileged material apply: Interception CoP §9.62; Bulk EI CoP §9.58.

[24] i.e. where the British Islands safeguard applies (and other "selection criteria" do not authorise selection for examination): see s.152(3)(d) (bulk interception), s.193(3)(d) (bulk equipment interference).

c. In the event that privileged communications are inadvertently and unexpectedly selected for examination (so that the enhanced procedure has not been followed), any content so obtained must be handled strictly in accordance with ss.153/194, and the applicable provisions of the Codes, and no further privileged material may be intentionally selected for examination by reference to those criteria unless approved by a senior official: Interception CoP §9.61; EI CoP §9.57.

d. An authority will not act on or further disseminate legally privileged items without first informing the IPC that the items have been obtained or selected for examination, save where there is an urgent need to take action and it is not reasonably practicable to inform the IPC. In such cases, the agency should wherever possible consult a legal adviser. See Interception CoP §9.71; EI CoP §9.67.

Journalists: bulk interception and bulk EI

52. Relevant statutory safeguards apply to (i) "confidential journalistic material" (as defined in s.264[25]); and (ii) "sources of journalistic information" (as defined in s.263).

53. In relation to confidential journalistic material, where such material is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the IPC as soon as is reasonably practicable: ss.154, 195.

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that require reporting to the IPC where "*confidential journalistic material*" is retained (ss 154 and 195) do not prohibit the use of dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

54. Additional statutory safeguards apply where a targeted examination warrant is required[26] and the (or a) purpose is the selection for examination of "*journalistic material*" which the authority believes is "*confidential journalistic material*". The warrant application must contain a statement that the purpose is to select such material for examination; and the person to whom the application is made may issue the warrant only if they consider that the arrangements under s.150 or s.191 (as the case may be) include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material: see s.28(2), s.113.

55. The same applies, *mutatis mutandis*, where an application is made for a targeted examination warrant for the (or a) purpose of identifying a source of journalistic information i.e. the application must so state; and the person issuing the warrant must consider that appropriate arrangements are in place: s.29, s.114.

[25] S.264 contains statutory definitions of "*journalistic material*" and "*confidential journalistic material*".
[26] i.e. where the British Islands safeguard applies (and none of the other "*selection conditions*" is met).

56. Under the Codes:

a. Where an authorised person intends to select content or secondary data for examination in order to identify or confirm a source of journalistic information (and where it is not necessary to apply for a targeted examination warrant) s/he must notify a senior official[27] before so doing, and may not select the material for examination unless s/he has received the official's approval. The senior official may not provide such approval unless s/he considers that the agency has arrangements in place for the handling, retention, use and destruction of communications that identify sources of journalistic information. The same applies to the selection for examination of content in order to obtain confidential journalistic material. See Interception CoP §§9.84-9.86; Bulk EI CoP §§9.84-9.86.

b. Where confidential journalistic material, or material identifying a journalistic source, is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated information as confidential: Interception CoP §9.87; Bulk EI CoP, §9.80.

c. The EI Code provides that where an application is made for a targeted examination warrant to identify a source, the *"public interest requiring such selection must override any other public interest"*: EI Code, §9.76.

Bulk Acquisition: lawyers and journalists

57. The Bulk Acquisition CoP contains specific protections for the selection of data for examination in such cases:

a. The Bulk Acquisition CoP requires officers to take into account any circumstances that might lead to an unusual degree of intrusion when selecting data for examination. Such circumstances are specifically stated to include *"all cases where it is intended or known that the data being selected for examination includes communications data of…lawyers, journalists…"*: §6.23.

b. Further provision is made as to journalists:

i. The selection for examination of data in order to determine a source of journalistic information requires prior approval from a person holding the rank of Director or above, and any communications data so obtained and retained must be notified to the IPC at the next inspection: §6.28. This does not apply where the intent is to examine a journalist's communications data but not intended to determine the source of journalistic information: §6.30.

ii. Further, where a journalist's data is selected, but the intention is not to determine a source of journalistic information, particular care must be taken to ensure that

[27] As defined in s.145.

the officer considers whether the intrusion is justified, giving proper consideration to the public interest, and whether there are alternative means for obtaining the information: §6.31.

(iv) Offences

58. The Act creates specific criminal offences that apply where a person deliberately selects material for examination that breaches the examination safeguards referred to above, knowing or believing that doing so will breach the safeguard: see ss.155, 173, 196. Such an offence is punishable on conviction on indictment by imprisonment for up to 2 years or an unlimited fine.

(h) Requirement for independent approval of warrants by a Judicial Commissioner

(i) General position (non-urgent warrants)

59. In the case of all three types of bulk warrant in Part 6, the Secretary of State's power to issue a warrant is subject to a requirement to obtain independent approval by a Judicial Commissioner (ss.140, 159, 179). The Judicial Commissioner is required to review the Secretary of State's conclusions as to:

    a. whether the warrant is necessary, by reference to the purpose for which the warrant is sought (e.g. national security);

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

    c. Whether each of the specified operational purposes is a purpose for which the examination of the content/data obtained is or may be necessary;

    d. Whether the examination of content/data for each purpose is necessary on any of the grounds on which the Secretary of State considered the warrant to be necessary.

60. The Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review and must consider matters with a sufficient degree of care as to ensure that s/he complies with the general duties in relation to privacy imposed by s.2.

61. Where a Judicial Commissioner refuses to approve a decision to issue a warrant, s/he must give written reasons to the Secretary of State, and the Secretary of State may in that case ask the IPC (unless he was the Judicial Commissioner who gave the refusal) to decide whether to approve the decision to issue the warrant.

(ii) Judicial Commissioner approval of bulk equipment interference warrants in urgent cases

62. As set out above, in relation to bulk equipment interference warrants only, the Secretary of State is not required to obtain advance approval from a Judicial Commissioner in urgent cases: s.178(1)(f).

63. In such a case, the Secretary of State must inform a Judicial Commissioner that a warrant has been issued, following which that Judicial Commissioner must (before the end of the third working day after the day on which the warrant was issued) decide whether to approve the decision to issue the warrant, and notify the Secretary of State of that decision. If the Judicial Commissioner refuses to approve the decision, the warrant ceases to have effect (unless already cancelled) and may not be renewed: s.180. Where this occurs, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible: s.181(2). The Judicial Commissioner may (a) authorise further interference with equipment for the purpose of enabling the person to secure that anything in the process of being done under the warrant stops as soon as possible, (b) direct that any material obtained under the warrant is destroyed; and/or (c) impose conditions as to the use or retention of any of that material: s.181(3). In exercising these functions, the Judicial Commissioner may require an 'affected party' (being both the Secretary of State and the addressee of the warrant) to make representations, and must have regard to any representations made by an affected party (whether or not such representations were required): ss.181(4)-(5).

64. The Secretary of State may ask the IPC to review a decision made by any other Judicial Commissioner under s.181(3), whereupon the IPC may confirm the decision or make a fresh one: s.181(7).

65. Nothing in ss.180 or 181 affects the lawfulness of anything done under a warrant before it ceases to have effect, or anything being done under a warrant when it ceases to have affect before that thing could be stopped or that it is not reasonably practicable to stop: s.181(8).

(i) **Duration, modification and cancellation of bulk warrants**

66. As to duration, bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants (unless already cancelled) cease to have effect at the end of the period of 6 months beginning with (a) the day on which the warrant was issued, or (b) 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: ss.143, 162, 184(1) and (2)(b)[28].

67. As to renewal, the Secretary of State may renew a bulk interception warrant, bulk acquisition warrant or a bulk equipment interference warrant at any time during the period of 30 days ending with the day at the end of which the warrant concerned would otherwise cease to have effect, provided that certain "*renewal conditions*" are met. The relevant renewal conditions in each case are as follows:

> "*(a) that the Secretary of State considers that the warrant continues to be necessary—*
>
> *(i) in the interests of national security, or*
>
> *(ii) on that ground and on any other grounds falling within* section 138(2),

[28] Save that in relation to an 'urgent' bulk equipment interference warrant (i.e. one issued without advance Judicial Commissioner approval: see above), the warrant ceases to have effect at the end of the period ending with the fifth working day after the day on which the warrant was issued.

> *(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,*
> *(c) that the Secretary of State considers that—*
> *(i) each of the specified operational purposes (see* section 142*) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant continues to be, or may be, necessary, and*
> *(ii) the examination of intercepted content or secondary data for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and*
> *(d) that the decision to renew the warrant has been approved by a Judicial Commissioner*."
>
> (ss.144, 163 and 185 of the Act)

68. As to modification, the provisions of bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants may be modified at any time in order to add, vary or remove any specified operational purpose or to provide that the warrant no longer requires or authorises specified activities: ss.145, 164 and 186. The addition or variation of a specified operational purpose is designated as a "*major*" modification, which is subject to a separate requirement for Judicial Commissioner approval (except in urgent cases, where Judicial Commissioner approval of a major modification must be sought and obtained within three working days): ss.145(5), 146- 147; ss.164(5), 165-166; ss.186(6), 187-188.

69. As to cancellation, the Secretary of State (or a senior official acting on his/her behalf) may cancel a bulk interception warrant, bulk acquisition warrant or bulk equipment interference warrant at any time. Moreover, s/he must cancel such a warrant where certain conditions are met, *viz.* that the warrant is no longer necessary in the interests of national security[29], the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct, or the examination of material obtained under the warrant is no longer necessary for any of the specified operational purposes (ss.148, 167, 189). Where a warrant is cancelled, the addressee of the warrant must, so far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible (ss.148(5), 167(5) 189(5)). A warrant that has been cancelled may not be renewed (ss.148(6), 167(6) and 189(6)).

III) TARGETED/THEMATIC EQUIPMENT INTERFERENCE WARRANTS UNDER PART 5

70. In addition to the bulk powers in Pt 6 Chs 1–3 of the Act, this claim concerns the lawfulness of aspects of the equipment interference regime in Part 5 of the Act.

[29] Save that this cancellation condition does not apply where the warrant has been modified so that it no longer authorises or requires: the interception of communications/obtaining of secondary data (in the case of a bulk interception warrant), the requiring of a telecommunications operator to disclose, or obtain and disclose, communications data specified in the warrant (in the case of a bulk acquisition warrant) or the securing of interference with any equipment or the obtaining of any communications, equipment data or other information (in the case of a bulk equipment interference warrant): ss.148(4), 167(4) and 189(4).

71. The only aspects presently in issue are the provisions described in the Act as "*targeted equipment interference warrants*" (being warrants which authorise or require the addressee to secure interference with any equipment for the purpose of obtaining communications, equipment data or any other information (s.99(2)) where the subject matter of warrant falls within s.101(1)(b)-(h) of the Act (commonly referred to as "*thematic equipment interference warrants*")[30]:

> "*…(b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;*
> *(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;*
> *(d) equipment in a particular location;*
> *(e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;*
> *(f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;*
> *(g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;*
> *(h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment*."

72. Several of the requirements for the issue of a targeted/thematic equipment interference warrant are similar to those that apply in relation to bulk warrants under Pt 6 Chs 1-3 (see above).

73. Thus, following an application made by an intelligence service, the Secretary of State may issue a targeted/thematic equipment interference warrant if:

    a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, (ii) for the purpose of preventing or detecting serious crime or (iii) in the interests of the economic well-being of the United Kingdom, so far as those interests are also relevant to the interests of national security (s.102(1)(a) and (5)). A targeted/thematic warrant may be issued for any of these purposes.

    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 (s.102(1)(b)).

    c. The Secretary of State considers that satisfactory safeguards are in force in relation to the warrant pursuant to ss.129 and 130 (s.102(1)(c)). Those safeguards (concerning retention and disclosure of material, and the disclosure of material to overseas authorities) are essentially equivalent to those that apply in relation to bulk warrants, save that, given the 'non-bulk' nature of the material obtained under targeted equipment interference warrants, there is no process of 'selection for examination' of material obtained pursuant to a targeted equipment interference

[30] At this stage, Liberty does not ask the Court to rule on the lawfulness of a targeted examination warrant whose subject matter is as specified in s.101(1)(a) of the Act, i.e. "*equipment belonging to, used by or in the possession of a particular person or organisation*".

warrant, and therefore no 'examination safeguards' applicable to that process.[31]

d. Except in urgent cases, the decision to issue the warrant has been approved by a Judicial Commissioner (s.102(1)(d)). The provisions for Judicial Commissioner approval, and for retrospective approval or refusal in urgent cases, in ss.108-110 match those in relation to bulk equipment interference warrants (see above).

74. Additional safeguards apply where the purpose of an equipment interference warrant is to obtain items subject to legal privilege: s.112 of the Act. These mirror the safeguards applicable to the selection for examination of material obtained under a bulk warrant (see e.g. s.153 in relation to bulk interception warrants).

75. Further, where an application is made for a targeted equipment interference warrant and the purpose, or one of the purposes of the warrant, is to obtain confidential journalistic material or to identify / confirm a source of journalistic information, the application must contain a statement to that effect and a warrant may be issued only if specific arrangements are in place for the handling, retention, use and destruction of communications or other items of information containing such material: ss.113 – 114.

76. In contrast to the bulk powers, Part 5 of the Act also makes provision for the issue of targeted equipment interference warrants by the Scottish Ministers (s.103), by the Secretary of State to the Chief of Defence Intelligence (s.104) and by certain "*law enforcement chiefs*" to appropriate law enforcement officers (s.106-107). The requirements for the issue of warrants in these instances are similar, but not identical, to the requirements in s.102 of the Act (issue of a targeted equipment interference warrant by the Secretary of State to the head of an intelligence service).

77. S.115 of the Act makes detailed provision for, inter alia, the details that must be included in a targeted equipment interference warrant, which depends on the subject matter of the warrant. For instance, where the subject matter of such a warrant is equipment belonging to (etc.) persons who form a group which shares a common purpose or carries on a particular activity, the warrant must contain a description of the purpose / activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe: s.115(3).

78. Sections 116-125 make detailed provision for the duration, renewal, modification and cancellation of warrants (including targeted equipment interference warrants) issued under Pt 5 of the Act.

IV) BULK PERSONAL DATASET WARRANTS — PART 7

79. Under s.199(1) of the Act, an intelligence service retains a bulk personal dataset ("**BPD**") where: (a) it 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

[31] As with the bulk powers, there are also enhanced safeguards in relation to the retention of legally privileged material obtained pursuant to a targeted equipment interference warrant (s.131 of the Act).

not, and are unlikely to become, of intelligence interest; (c) after any initial examination[32] of the content, the intelligence service retains the set of information for purpose of the exercise of its functions; and (d) the set is held, or to be held, electronically for analysis in the exercise of those functions.[33]

80. An intelligence service may not exercise a power to retain a BPD unless its retention is authorised by either a "*class BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD of a class described in the warrant) or a "*specific BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD described in the warrant): s.200.

81. Part 7 does not itself contain any power to obtain a BPD. Rather, the requirement for a BPD warrant concerns the retention and any subsequent examination of a BPD obtained by other means. Such means may include a warrant issued under s.5 of the Intelligence Services Act 1994 ("**ISA**"), other exercise of the intelligence services' "information gateway" powers under the ISA and Security Service Act 1989, and the other powers under the Act (except for Pt 6 Ch 2).

82. In the case of both a class BPD warrant and a specific BPD warrant, the decision to issue must be taken by the Secretary of State personally: s.211.

83. The requirement for the authorisation of retention of a BPD by way of a warrant under s.200 does not apply where an intelligence service exercises a power to retain or examine a BPD obtained under a warrant or other authorisation issued or given under the 2016 Act itself: s.201(1). However, as discussed below, the Secretary of State may direct that material so obtained should instead be treated as a BPD subject to the provisions of Pt 7.

(a) Class BPD warrants

84. On an application by the head of an intelligence service (or a person acting on his or her behalf), the Secretary of State may issue a class BPD warrant if (see s.204):

    a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, or (ii) for the purposes of preventing or detecting serious crime, or (iii) in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security (s.204(3)(a));

    b. The Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct (s.204(3)(b));

    c. Where the warrant authorises the examination of BPDs of the class described in the warrant, the Secretary of State considers that (i) each of the specified operational purposes is a purpose for which the examination of BPDs of that class is or may

[32] Section 220 provides for time limits on the initial examination of a set of information to determine whether it constitutes a BPD within the meaning of s.199 and, if so to seek a class or specific BPD warrant. Broadly speaking, the head of an intelligence service has 3 months to do so where the set of information was created in the UK, and 6 months where it was created outside the UK.

[33] "*Personal data*" means (a) data within the meaning of s.3(2) of the Data Protection Act 2018 (i.e. relating to an identified or identifiable living individual) which is subject to processing described in s.82(1) of that Act (processing by an intelligence service of personal data wholly or partly by automated means, etc.), or (b) data relating to a deceased individual which would fall within (a) if it related to a living individual.

be necessary, and (ii) the examination of BPDs of that class for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (s.204(3)(c)(i) and (ii)). S.212 makes further provision for the specification of operational purposes in a warrant, in terms which mirror the provisions of s.142 of the Act in relation to bulk interception warrants and the equivalent provisions relating to bulk acquisition warrants and bulk equipment interference warrants.

d. The Secretary of State considers that the arrangements made by the intelligence service for storing BPDs of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory (s.204(3)(d)).

e. The decision to issue the warrant has been approved by a Judicial Commissioner (s.204(3)(e)). See s.208 for the provision as to Judicial Commissioner approval.

85. A BPD may not, however, be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of or includes, "*protected data*"[34] or "*health records*"[35] or that a substantial proportion of the BPD consists of "*sensitive personal data*"[36]: s.202(1) and (2).

86. Further, an intelligence service may not retain, or retain and examine, a BPD pursuant to a class BPD warrant if the head of the intelligence service considers that the nature of the BPD or the circumstances of its creation are such that its retention, or retention and examination, raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application for a specific BPD warrant.

(b) Specific BPD warrants

87. A specific BPD warrant may be sought by the head of an intelligence service (or a person acting on his or her behalf) where (see s.205(1)-(3)):

a. the BPD does not fall within a class described in a class BPD warrant; or

b. The BPD falls within a class described in a class BPD warrant but the intelligence service is prevented from retaining, or retaining and examining, it in reliance on the class BPD warrant by virtue of the restrictions in s.202 (see above) *or* that intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

[34] Defined in s.203 as any data contained in a BPD other than systems data (see above), identifying data (see above) which is contained in the BPD which is capable of being logically separated from the BPD and if so separated would not reveal anything of what might reasonably be considered to be the meaning of the remaining data, and data which is not private information (which includes information relating to a person's private or family life).

[35] Defined in s.202(4) read with s.206(6) as a record, or copy of a record, which consists of information relating to the physical or mental health or condition of an individual, was made by or on behalf of a health professional in connection with that individual's care, and was obtained by the intelligence service from a health professional or a health service body (or from a person acting on their behalf).

[36] Meaning personal data consisting of information about an individual (whether living or deceased) or a kind mentioned in s.86(7)(a)-(e) of the Data Protection Act 2018 (covering matters such as personal data revealing political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, and so on).

88. Subject to those points, the basic criteria for the issue of a specific BPD warrant by the Secretary of State are the same as those for the issue of a class BPD warrant, save that advance Judicial Commissioner approval need not be obtained in urgent cases: see s.205(6)(a)-(e). Provision for *post hoc* Judicial Commissioner approval of specific BPD warrants in urgent cases is made at ss.209 – 210 (in terms which mirror the provision for such approval in relation to bulk equipment interference warrants in urgent cases).

89. Additional safeguards apply to applications for specific BPD warrants in relation to:

    a. Health records: Section 206(1)-(3) provides that the Secretary of State may only issue a specific BPD warrant the purpose (or one of the purposes) of which is to authorise the retention, or retention and examination, of health records in "*exceptional and compelling circumstances*". Section 206(4)–(5) provides that, where the head of an intelligence services considers that a BPD includes or is "*likely*" to include health records (but it is not a or the purpose of a warrant to retain them), then the application must contain a statement to that effect.

    b. Protected data: Section 207 provides that, where the Secretary of State decides to issue a specific BPD warrant, s/he may impose conditions which must be satisfied before "*protected data*" (see s.203, considered at fn 34 above) retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.

(c) Duration, renewal, modification and cancellation of BPD warrants

90. Sections 213-219 make provision for the duration, renewal, modification and cancellation of BPD warrants. The provision made largely mirrors the provision for the duration, etc., of bulk warrants under Pt 6 Chs 1-3 (including the requirement for Judicial Commissioner approval of "*major modifications*").

91. One different provision is s.219, which provides that, where a BPD warrant ceases to have effect because it expires without having been renewed or is cancelled:

    a. Within five working days after the expiry or cancellation of a BPD warrant, the head of the intelligence service to whom the warrant was addressed may either:

        i. apply for a specific or class BPD warrant authorising the retention, or retention and examination, of the whole or any part of the material previously retained pursuant to a BPD warrant (in which case the usual criteria for the grant of such an application will apply) (s.219(2)(a)); or

        ii. where the head of the intelligence service wishes to give further consideration to whether to apply for a further specific / class BPD warrant, apply to the Secretary of State for authorisation to retain / examine the whole or any part of the material retained in reliance on the warrant (s.219(2)(b)).

b. Where an application is made to the Secretary of State, s/he may direct that any of the material to which the application relates be destroyed (s.219(3)(a)), or (with the approval of a Judicial Commissioner) authorise the retention, or retention and examination, of any of that material, subject to such conditions as s/he considers appropriate, for a specified period not exceeding 3 months (s.219(3)(b)).

c. During that period, the head of an intelligence service may apply for a BPD warrant and must do so as soon as practicable and before the end of that period (s.219(7)).

d. S.219(8) provides that an intelligence service does not breach s.200 by virtue of its retention or examination of material to which a BPD warrant related where that intelligence service is seeking a further warrant or authorisation pursuant to s.219 during the periods mentioned above, as follows:

i. "*First period*": Five working days from when the BPD warrant cases to have effect;

ii. "*Second period*": The period beginning with the day of any application under s.219(2)(a) or (b) and ending with its determination;

iii. "*Third period*": The period during which retention or examination is authorised under s.219(3)(b) (at most three months);

iv. "*Fourth period*": Where an authorisation under s.219(3)(b) is given and the head of an intelligence service then makes an application under s.219(7) for a BPD warrant, the period beginning with the expiry of the authorisation under s.219(3)(b) and the determination of the application.

(d) Safeguards relating to the examination of BPDs

92. S.221 requires the Secretary of State to ensure that arrangements are in force for securing that:

a. any selection for examination of data contained in BPDs is carried out only so far as is necessary for the operational purposes specified in the warrant (at the time of the selection); and

b. the selection of any such data is necessary and proportionate in all the circumstances.

93. The Secretary of State must also ensure, in relation to every specific BPD warrant in which conditions in relation to the selection for examination of data under s.207 (see above) are imposed, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant.

94. As with the bulk powers in Pt 6 Chs 1-3, enhanced safeguards apply to the selection for examination pursuant to a specific BPD warrant of items subject to legal privilege (which differ depending on whether it is the / a purpose of the warrant to obtain privileged items, this is likely, or the addressee of a warrant considers that the data is not privileged because it or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose): s.222.

95. It is a criminal offence, punishable on conviction on indictment by a prison term of up to 2 years or an unlimited fine, to deliberately select data for examination under a class BPD warrant or a specific BPD warrant, knowing or believing that the selection of that data is in breach of certain specified safeguards (e.g. that any such selection is carried out only so far as is necessary for the operational purposes specified in the warrant, and so on): s.224.

(e) Application of Pt 7 to BPDs obtained under other powers in the Act

96. Section 225 provides that the Secretary of State may, on an application by the head of the intelligence service, give a direction that the intelligence service may retain, or retain and examine, a BPD that has been obtained under a warrant issued under another provision of the Act (except a bulk acquisition warrant under Pt 6 Ch 2). In such a case, the power under which the BPD was obtained ceases to apply, and the intelligence service thereafter requires the authorisation of either a class BPD warrant or a specific BPD warrant. Such a direction may provide for any "*associated regulatory provision*" specified in the direction to continue to apply in relation to the BPD (meaning any provision which is made by or for the purposes of the Act (other than Pt 7) that applied immediately prior to the direction). A direction under s.225 may only be given with the approval of a Judicial Commissioner, and it may not be revoked (it may be varied, but only for the purpose of altering or removing any provision included in the direction).

V) ACQUISITION AND RETENTION OF COMMUNICATIONS DATA – PTS 3 AND 4 OF THE ACT

97. Parts 3 and 4 of the Act were the subject matter of the February 2018 hearing. However, certain amendments to those Parts of the Act have taken effect since the Court gave its judgment in these proceedings on 27 April 2018.

98. Part 4 relates to the procedure for requiring telecommunications providers to *retain* communications data and Part 3 relates to the procedure for authorisation for relevant public authorities to *obtain* communications data. Those Parts of the Act are supplemented by the Communications Data Code of Practice (November 2018) (the "**CD CoP**"), which provides guidance on the procedures to be followed when acquisition of communications data takes place under Part 3 and when communications data is retained under Part 4.

(a) Retention of communications data – Part 4

99. Section 87 provides that the Secretary of State may, by notice (a "*retention notice*") require a telecommunications operator to retain relevant communications data if (a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the

specified purposes and (b) the decision to give the notice has been approved by a Judicial Commissioner.

100. Since the Court's judgment in February 2018, the specified purposes (in s.87(1)) have been amended[37]. They are now restricted to retention that is necessary and proportionate: (i) in the interests of national security, (ii) for the applicable crime purpose (see s.87(10A)), 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,
(iv) in the interests of public safety, (v) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, and (vi) to assist investigations into alleged miscarriages of justice. The crime purpose for which events data (such as call histories and location information) can be retained and acquired is restricted to 'serious crime', whereas entity data (such as the name of a subscriber to a service) can be obtained in relation to the full range of crimes. The provisions requiring approval of retention notices by a Judicial Commissioner have now come into force.[38]

101. As the Court noted in paragraphs [129] to [138] of its 27 April 2018 judgment:

a. s.87(2) provides, *inter alia*, that a notice may relate to a "description of data", may relate to a particular operator or to a description of operators, and that a retention notice may specify the period of time for which data is to be retained, which may not exceed 12 months;

b. before the Secretary of State may serve a retention notice, s/he must have regard to, among other matters, the factors listed in s.88(1), which comprise the likely benefits of serving the notice, the number of users to which the notice relates, the technical feasibility and costs of complying with the notice and any other effect on the telecommunications operator to be served;

c. a retention notice may not be given unless the Secretary of State's decision has been approved by a Judicial Commissioner under s.89, requiring a review of whether the requirements in the proposed notice are necessary and proportionate, applying the same principles as would be applied in judicial review, and ensuring that his or her consideration is sufficiently careful so as to comply with the duties in s.2 of the Act;

d. a telecommunications operator which receives a retention notice may refer the notice back to the Secretary of State for a formal process of review, in accordance with ss.90 to 91. These provisions are now fully in force and require the Secretary of State to consult and take into account the report of a Technical Advisory Board and a Judicial Commissioner (s.90(6), (9) and (10)). The Secretary of State may not vary or confirm a notice (as opposed to revoking a notice) unless that decision is approved by the IPC (s.90(11)).

[37] By the Data Retention and Acquisition Regulations 2018 (SI 2018/1123, 1 November 2018).
[38] Pursuant to reg. 4(a) of the Investigatory Powers Act 2016 (Commencement No. 7 and Transitional and Saving Provisions) Regulations 2018/873

(b) Acquisition of communications data – Part 3

102. Applications to *acquire* communications data can be authorised by three separate categories of individual, depending on the circumstances:

a. s.60A of the Act confers power on the IPC to authorise applications for communications data in relation to the purposes set out in s.60A(7), i.e: (a) national security; (b) the applicable crime purpose (see s.60A(8)); (c) the economic well-being of the United Kingdom so far as relevant to the interests of national security; (d) public safety; (e) preventing death or injury or any damage to physical or mental health, or mitigating any injury or damage to physical or mental health; (f) assisting investigations into alleged miscarriages of justice, or (g) identifying dead or incapacitated persons;

b. s.61 provides for the authorisation of communications data requests relating to national security. Where an application for communications data is for the purpose of national security under s.61(7)(a), or economic well-being where relevant to national security under s.61(7)(c), or where it is an application made by a member of an intelligence agency under s.61(7)(b) (the applicable crime purpose), an application may, as an alternative to IPC authorisation under s.60A, be authorised internally by a designated senior officer in the public authority. The designated senior officer must, except where provided for in the Act, be independent of the operation concerned (see s.63(1));

c. s.61A provides for designated senior officers to grant authorisations in urgent cases. Examples of urgent circumstances, including an immediate threat of loss or serious harm to human life, an urgent operational requirement for data that will directly assist the prevention or detection of the commission of a serious crime or a credible and immediate threat to national security, are set out in CD CoP §5.31.

103. Under s.60A(1), the IPC may grant an authorisation, on an application made by a relevant public authority, where he considers that: (a) it is *necessary* for the relevant public authority to obtain communications data for a specified purpose falling within subsection 60A(7); (b) it is *necessary* for the relevant public authority to obtain the data
(i) for the purposes of a specific investigation or a specific operation or (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data; and (c) that the conduct authorised by the authorisation is *proportionate* to what is sought to be achieved.

104. Similar conditions of necessity and proportionality apply for authorisations under s.61 and 61A (with the additional requirement of urgency in s.61A).

105. Ss.62-66 have been moved and grouped together under a new heading "*Further provision about authorisations*". They impose additional restrictions on acquisition of communications data, including:

a. Preventing local authorities from acquiring internet connection records for any purpose, and restricting the ability of other public authorities to access internet connection records to specific circumstances and purposes. This imposes a requirement for additional consideration of the proportionality of the application

in relation to the level of processing and disclosure involved (see s.62 and CD CoP, Part 9);

b. Restricting the ability of designated senior officers to grant an authorisation if the officer is working on the relevant investigation or operation (s.63);

c. Specifying the content of authorisations (s.64);

d. Limiting the duration of authorisations (to one month, or 3 days in the case of urgent authorisations), subject to renewal or cancellation (s.65); and

e. Imposing duties on telecommunications providers, including a duty to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned (s.66).

106. Further safeguards are put in places by ss.76 and 77, in particular:

a. A requirement (subject to certain exceptions) to consult a person who is acting as a single point of contact in relation to the making of applications, before making any application to IPCO for authorisation under s.60A, or before a designated senior officer grants authorisation under s.61 or s.61A. Such consultation may encompass questions relating to the most appropriate methods for obtaining data, any unintended consequences of the proposed authorisation, and any issues as to the lawfulness of the proposed authorisation; and

b. A requirement for Judicial Commissioner approval for authorisations under s.61 or s.61A (or delegated decisions made under s.60A) to identify or confirm journalistic sources, where the authorisation is not necessary because of an imminent threat to life. S.77(6) requires, in particular, that the Judicial Commissioner must have regard to— (a) the public interest in protecting a source of journalistic information, and (b) the need for there to be another overriding public interest before a relevant public authority seeks to identify or confirm a source of journalistic information. This provision is supplemented by the CD CoP, §§8.23ff.

(c) RIPA Part 1 Chapter 2

107. The regime for the acquisition of communications data under Regulation of Investigatory Powers Act 2000 Pt 1 Ch 2 has not yet been repealed. It operates alongside IPA Pts 3–4 for some public authorities. The provisions have been amended to provide that "*traffic data*" and data about the use of any postal service, telecommunication service or part of a telecommunication system (see s.21(4)(a)-(b)) can only be acquired in relation to "*serious crime*".

VI) OVERSIGHT ARRANGEMENTS – PART 8 OF THE ACT

108. Part 8 makes provision for a series of oversight arrangements in relation to the exercise of the range of investigatory powers under the Act. In particular, Part 8:

a. provides for the appointment of a new IPC (the Investigatory Powers Commissioner) and other Judicial Commissioners; and

b. provides for the jurisdiction of the (existing) Investigatory Powers Tribunal ("**IPT**") in respect of the use of investigatory powers under the Act and introduces a new right of appeal against the IPT's decisions.

(a) The IPC and the Judicial Commissioners

109. The IPC replaces and consolidates the functions of a series of pre-existing oversight bodies, all of which were all abolished by the Act: s.240.

110. Section 227(1) requires the Prime Minister to appoint the IPC and such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the Judicial Commissioners' functions. The IPC and the Judicial Commissioners must hold or have held a high judicial office: s.227(2). The current (and first) IPC is the Rt Hon Lord Justice Fulford (appointed February 2017). His Deputy is the Rt Hon Sir John Goldring. The IPC is supported in his role by the Office of the Investigatory Powers Commissioner ("**IPCO**"). S.238 of the Act makes general provision for funding, staff and facilities in relation to the IPC and the Judicial Commissioners.

111. The IPC's main oversight functions are set out in s.229, and include (so far as is material):

a. keeping under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to *inter alia* the interception of communications, the acquisition and retention of communications data and equipment interference: s.229(1)-(2);

b. keeping under review (including by way of audit, inspection and investigation) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service: s.229(3)(a);

c. keeping under review the operation of safeguards to protect privacy: s.229(5).

(i) Error reporting and notification to victims

112. Under s. 235(6) a public authority, telecommunications operator or postal operator must report to the IPC any "*relevant error*" (as defined in s. 231(9)). A "*relevant error*" means an error (a) by a public authority in complying with any requirements which are imposed on it by virtue of the 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 specified under Schedule 7: s.231(9). The IPC must also keep under review the definition of "*relevant error*": s.231(9).

113. Under the Interception CoP §10.17, EI CoP §10.19, Bulk Acquisition CoP §10.15 and BPD CoP §8.11, relevant errors must be notified to the IPC "*as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred*". Under CD CoP §24.26, the requirement is to report the error to the authority's senior responsible officer and then to the IPC "*within no more than five working days of it being established that an error has occurred*".

114. Under s.231(1) of the Act, the IPC must[39] 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[40]. The IPC may not decide that an error is serious unless he considers that the error has caused significant prejudice or harm to the person concerned: s.231(2). The fact that there has been a breach of a person's Convention rights is not sufficient by itself to amount to a serious error: s.231(3).

115. When informing someone of an error, the IPC must also (s.231(6)):

> *"(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)."*

(ii) Annual reporting by the IPC

116. The IPC must also, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the Judicial Commissioners (s.234(1)), including the detailed matters specified in s.234(2), which include statistics on the use of investigatory powers, information about the results and impact of such use, information about the operation of the safeguards under the Act, and so on. A report under s.234(1) must also include information about the number of relevant errors of which the IPC has become aware during the year to which the report relates, the number of such errors which the IPC has decided were serious errors, and the number of persons who have been informed of such errors: s.231(8).

117. On receipt of a report from the IPC under s.234(1), the Prime Minister must publish the report and lay a copy before Parliament: s.234(6)[41]. The IPC also has a discretion, where he considers it appropriate, to make a report to the Prime Minister on any matter relating to the functions of the Judicial Commissioners: s.234(4). A report under s.234(1) or (4) may, in particular, include such recommendations as the IPC considers appropriate about any matter relating to the functions of the Judicial Commissioners. The IPC is also required to make any report to the Prime Minister which the Prime Minister has requested: s.234(3).

(iii) Judicial Commissioners' functions

118. The main relevant functions of Judicial Commissioners under the Act concern the giving of authorisations for warrants and notices issued by the Secretary of State in respect of

[39] Having first given the public authority which has made the error the opportunity to make submissions: s.231(5).
[40] In deciding this, the IPC must consider, in particular "*(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*".
[41] S.231(7) provides that, on consultation with the IPC, the Prime Minister may exclude from the published version of the report any part of the report that would be contrary to the public interest or prejudicial to national security or other matters specified in s.231(7)(a)-(d).

the exercise of the various investigatory powers in the Act: see above. However, they also have a number of more general duties and powers under Part 8 of the Act.

119. Under s.229(6)-(7), when exercising functions under the Act, a Judicial Commissioner must not act in a way that s/he considers to be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the economic well-being of the United Kingdom, and must in particular ensure that the Commissioner does not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, or unduly impede the operational effectiveness of an intelligence service, police force, government department or Her Majesty's forces. However, these general duties do not apply in relation to certain of the Judicial Commissioners' functions, including deciding whether to approve the issue, modification or renewal of a warrant (s.229(8)(b)) and deciding whether to approve the grant, modification or renewal of a retention notice (s.229(8)(e)(i)).

120. Under s.235, the Judicial Commissioners have powers in relation to the carrying out of investigations, inspections and audits, including a power to obtain documents and information and to require assistance (including access to apparatus, systems, facilities and services) from "*relevant persons*", including any person who holds (or has held) an office, rank or position with a public authority and any telecommunications or postal operator who is, has been or may become subject to a requirement imposed by virtue of the Act (s.235(7)).

(b) **The IPT**

121. The Tribunal was established by s.65(1) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). Members of the Tribunal must either hold or have held high judicial office or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

122. The Tribunal has exclusive jurisdiction to consider claims under s.7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss.65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

123. The Tribunal may also consider and determine any complaints by a person who is aggrieved by certain conduct[42] which s/he believes to have taken place (in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system, and to have taken place in "*challengeable circumstances*" or to have been carried out by or on behalf of the intelligence services (ss.65(2)(b), 65(4) of RIPA). Conduct takes place in "*challengeable circumstances*" when either it is the conduct of a public authority and it takes place with the (purported) authority of (inter alia) a warrant under Pts 5, 6 or 7 of the 2016 Act, an authorisation or notice under Pt 3 of the 2016 Act, or a retention notice under Pt 4 of the 2016 Act, *or* the circumstances are such that it would not have been appropriate for the conduct to take place without at least

[42] A wide range of such conduct is specified in s.65(5) RIPA, and it includes the full panoply of actions that may be taken under the impugned parts of the 2016 Act.

proper consideration having been given to whether such authority should be sought (RIPA, ss.65(7) and (8)).

124. Any person, regardless of nationality, may bring a complaint to the Tribunal. The IPT considered the scope of its jurisdiction and the extent of the knowledge or evidence of the use of investigatory powers required to make a claim in *Human Rights Watch v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib_15_165-CH.

125. Complaints are investigated and then determined by the Tribunal "*by applying the same principles as would be applied by a court on an application for judicial review*" (s.67(3) of RIPA). S.68(6) of RIPA gives the Tribunal powers to order production of materials by, among others, every person holding office under the Crown. Further, under s.232(1) of the 2016 Act, a Judicial Commissioner must give the IPT all such documents, information and other assistance as the IPT may require in connection with the investigation, consideration or determination of any matter.

126. Subject to any provision in its rules, the Tribunal may — at the conclusion of a claim — make any such award of compensation or other order as it thinks fit, including, but not limited to, an order quashing or cancelling warrants, authorisations, notices and directions given under the 2016 Act and an order requiring the destruction of any records of information which have been obtained in exercise of any power conferred by a warrant, authorisation or notice under the Act, or which are held by any public authority in relation to any person: s.67(7) of RIPA.

127. S.242 of the 2016 Act introduced a new s.67A of RIPA, which provided (for the first time) for a right of appeal on a point of law from final decisions of the IPT which are not procedural to the Court of Appeal. A decision of the Tribunal is subject to judicial review: *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22.