Neutral Citation Number: [2022] EWHC 1630 (Admin)

Case No: CO/1052/2017

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 24 June 2022

Before :

LORD JUSTICE SINGH
and
MR JUSTICE HOLGATE

- -

Between :

THE QUEEN (on the application of NATIONAL COUNCIL FOR CIVIL LIBERTIES (LIBERTY))	**Claimant**
- and -	
(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT	**Defendants**
and	
(2) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS	

- -
- -

Ben Jaffey QC, David Heaton and Sophie Bird (instructed by **Bhatt Murphy**) for the **Claimant**
Sir James Eadie QC, Gerry Facenna QC, Julian Milford QC, Michael Armitage and John Bethell (instructed by **Treasury Solicitor**) for the **Defendants**

Hearing dates: 17-18 May 2022

- -

Approved Judgment

This judgment was handed down remotely by circulation to the parties' representatives by email and release to The National Archives. The date and time for hand-down will be deemed to be Friday 24th June 2022 at 10.30am. A copy of the judgment in final form as handed down can be made available after that time, on request by email to listoffice@administrativecourtoffice.justice.gov.uk;

Lord Justice Singh and Mr Justice Holgate:

Introduction

1. This is the third stage of the Claimant's challenge to provisions of the Investigatory Powers Act 2016 ("the IPA" or "the 2016 Act"). On 27 April 2018 we gave judgment on the first stage of the challenge, which concerned the compatibility of Part 4 of the IPA with European Union ("EU") law: [2018] EWHC 975 (Admin); [2019] QB 481 ("the 2018 judgment"). On 29 July 2019 we gave judgment in relation to the second stage of the challenge, which was an application for a declaration of incompatibility under section 4 of the Human Rights Act 1998 ("HRA"): [2019] EWHC 2057 (Admin); [2020] 1 WLR 243 ("the 2019 judgment"). This third stage of the challenge concerns the remaining EU law issues.

2. It is common ground before us that, although in the meantime the United Kingdom ("UK") has left the EU, on 31 January 2020, and the implementation period completion day has now passed (31 December 2020), relevant principles of EU law remain part of the law of this country as "retained EU law" under the European Union (Withdrawal) Act 2018 ("the 2018 Act"), as amended.

3. One reason why the residual EU law issues could not be determined in 2018 was that at that time there was pending a reference which had been made by the Investigatory Powers Tribunal ("IPT") to the Court of Justice of the European Union ("CJEU") in Case C-623/17 *Privacy International v Secretary of State for the Foreign and Commonwealth Office*. Judgment in that case was given by the Grand Chamber of the CJEU on 6 October 2020: [2021] 1 WLR 4421. On the same date the Grand Chamber gave judgment in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net & Ors v Premier Ministre & Ors*: [2021] 1 WLR 4457. Those two judgments have loomed large in the submissions for the Claimant before us.

4. Furthermore, significant reliance has been placed by the Claimant on the judgment of the Grand Chamber of the European Court of Human Rights ("ECtHR") in *Big Brother Watch & Ors v UK* (App. Nos. 58170/13, 62322/14 and 24960/15), which was delivered on 25 May 2021: (2022) 74 EHRR 17.

5. We are grateful to all counsel and those instructing them for the quality of their submissions, both written and oral. At the hearing before us we heard submissions by Mr Ben Jaffey QC on behalf of the Claimant and Sir James Eadie QC on behalf of the Defendants. After the hearing we received brief notes from each side, outlining their positions on the remedial powers which the Court might have should it decide any of the substantive issues in favour of the Claimant. It was agreed that further, more detailed submissions on remedies should await the outcome of the substantive claim.

The IPA

6. We summarised the legislative scheme of the IPA in the 2019 judgment, at paras. 34-62. We also set out an overview of the relevant legislation in an Annex to that judgment, which had been agreed between the parties, subject to three "riders" which were set out in the Annex. It is therefore unnecessary for us now to repeat what was

said in the 2019 judgment and the Annex, which should be treated as if they were incorporated into this judgment.

7. The issues which now arise before us fall broadly into two categories. First, the Claimant challenges aspects of Part 4 of the IPA, read with Part 3, which concerns "communications data". Secondly, the Claimant challenges aspects of the provisions in relation to "bulk powers", in Parts 5, 6 and 7 of the IPA.

Relevant EU legislation

8. The Claimant relies on the following provisions of the EU Charter of Fundamental Rights ("EU Charter"). Article 7 provides:

> "**Respect for private and family life**
>
> Everyone has the right to respect for his or her private and family life, home and communications."

9. Article 8 provides:

> "**Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

10. Article 11(1) provides:

> "**Freedom of expression and information**
>
> 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."

11. Article 51(1) provides:

> "**Field of application**
>
> 1. The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers."

12. Article 52 provides:

> "**Scope of guaranteed rights**
>
> 1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
>
> …
>
> 3. 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 and scope 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."

13. The Claimant also relies on Parliament and Council Directive 2002/58/EC (as amended by Parliament and Council Directive 2009/136/EC) ("the 'e-Privacy Directive'").

14. Article 1 of the e-Privacy Directive provides:

> "**Scope and aim**
>
> 1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

…

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

15. Article 3 provides:

"**Services concerned**

This Directive shall apply to the processing of personal data in connection with the provisions of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices."

16. Article 5(1) provides:

"**Confidentiality of the communications**

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

17. Article 15(1) provides:

"**Application of certain provisions of Directive 95/46/EC**

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary,

> appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

Procedural history

18. These judicial review proceedings were commenced on 28 February 2017 and have been considered by this Court in three stages.

19. The first stage of the claim was heard on 27-28 February 2018. This Court handed down its judgment on 27 April 2018, in which it held (as was conceded by the Defendants) that Part 4 of the IPA was incompatible with EU law in two respects, namely, that in relation to criminal justice:

    (1) access to and use of retained data was not limited to the purpose of preventing and detecting *serious* crime; and

    (2) access to retained data was not subject to prior *independent review*.

20. This Court stayed the proceedings on three further issues under EU law pending the judgment of the CJEU in the reference which had by then been made by the IPT in the case of *Privacy International*. The rest of the claim under EU law was dismissed.

21. This Court granted a declaration as to the law but stated that the Defendants would be given a reasonable period (approximately six months) to amend the incompatible legislation. The amendments to the IPA were made by secondary legislation: the Data Retention and Acquisition Regulations (SI 2018 No. 1123) ("the 2018 Regulations"), which came into force on 1 November 2018. We will address those amendments in greater detail below, since the Claimant does not accept that the amendments have fully satisfied the requirements of EU law.

22. On 27 November 2018 this Court granted the Claimant permission in respect of the rest of its claim. The order continued the stay of the proceedings insofar as they were based on EU law pending the judgment of the CJEU in *Privacy International*.

23. This Court heard the second stage of the claim on 17-21 June 2019, when it considered the claim based upon the European Convention on Human Rights ("ECHR") and, in particular, the application for a declaration of incompatibility under section 4 of the HRA. The Court gave judgment, refusing that application, on 29 July 2019. Subsequently, by agreement, the application for permission to appeal against

that decision was deferred until after the Grand Chamber of the ECtHR had given judgment in *Big Brother Watch v UK*: that judgment was given on 25 May 2021. Recently, on 28 April 2022, this Court granted permission to appeal on five grounds but refused permission on the sixth ground. That appeal is pending before the Court of Appeal.

24. On 6 October 2020 the CJEU handed down its judgment in *Privacy International* and, on the same date, in a set of cases to which we will refer as *La Quadrature*.

25. On 31 December 2020 the Claimant served its Re-re-amended Statement of Facts and Grounds, which took into account those two decisions of the CJEU.

26. On 19 February 2021 the Defendants served their Detailed Grounds of Resistance in respect of the remaining EU law matters in this case.

27. It is those remaining matters of EU law which are the subject of this judgment.

Retained EU law and its continued relevance

28. Since these proceedings were commenced the UK has left the EU. That process (often known as "Brexit") was achieved so far as domestic law is concerned by a number of statutes, in particular the 2018 Act. Section 1 of the 2018 Act repealed the European Communities Act 1972 from "exit day". The UK left the EU on 31 January 2020. There was, however, an "implementation period" or "IP", for which the completion day was 31 December 2020. The 2018 Act made provision both for what was to happen during the implementation period and after completion day.

29. Section 4 of the 2018 Act, so far as material provides:

> "(1) Any rights, powers, liabilities, obligations, restrictions, remedies and procedures which, immediately before IP completion day—
>
> (a) are recognised and available in domestic law by virtue of section 2(1) of the European Communities Act 1972, and
>
> (b) are enforced, allowed and followed accordingly,
>
> continue on and after IP completion day to be recognised and available in domestic law (and to be enforced, allowed and followed accordingly).
>
> (2) Subsection (1) does not apply to any rights, powers, liabilities, obligations, restrictions, remedies or procedures so far as they—
>
> (a) form part of domestic law by virtue of section 3,

> (aa) are, or are to be, recognised and available in domestic law (and enforced, allowed and followed accordingly) by virtue of section 7A or 7B, or
>
> (b) arise under an EU directive (including as applied by the EEA agreement) and are not of a kind recognised by the European Court or any court or tribunal in the United Kingdom in a case decided before IP completion day (whether or not as an essential part of the decision in the case)."

30. Section 5 of the 2018 Act provides:

> "(1) The principle of the supremacy of EU law does not apply to any enactment or rule of law passed or made on or after IP completion day.
>
> (2) Accordingly, the principle of the supremacy of EU law continues to apply on or after IP completion day so far as relevant to the interpretation, disapplication or quashing of any enactment or rule of law passed or made before IP completion day.
>
> (3) Subsection (1) does not prevent the principle of the supremacy of EU law from applying to a modification made on or after IP completion day of any enactment or rule of law passed or made before IP completion day if the application of the principle is consistent with the intention of the modification.
>
> (4) The Charter of Fundamental Rights is not part of domestic law on or after IP completion day.
>
> (5) Subsection (4) does not affect the retention in domestic law on or after IP completion day in accordance with this Act of any fundamental rights or principles which exist irrespective of the Charter (and references to the Charter in any case law are, so far as necessary for this purpose, to be read as if they were references to any corresponding retained fundamental rights or principles).
>
> …"

31. Section 6 of the 2018 Act provides:

> "(1) A court or tribunal—

> (a) is not bound by any principles laid down, or any decisions made, on or after IP completion day by the European Court, and
>
> (b) cannot refer any matter to the European Court on or after IP completion day.
>
> (2) Subject to this and subsections (3) to (6), a court or tribunal may have regard to anything done on or after IP completion day by the European Court, another EU entity or the EU so far as it is relevant to any matter before the court or tribunal.
>
> (3) Any question as to the validity, meaning or effect of any retained EU law is to be decided, so far as that law is unmodified on or after IP completion day and so far as they are relevant to it—
>
> (a) in accordance with any retained case law and any retained general principles of EU law, and
>
> (b) having regard (among other things) to the limits, immediately before IP completion day, of EU competences.
>
> …"

32. It is common ground that this Court does not have the power to depart from retained EU case law.

33. Part 4 of Sch. 8 to the 2018 Act contains specific transitional provisions, including provisions relating to the retention of saved EU law at the end of the implementation period. In particular para. 39(3) provides:

> "Section 5(4) … do[es] not apply in relation to any proceedings begun, but not finally decided, before a court or tribunal in the United Kingdom before IP completion date."

It is common ground that, since these proceedings were commenced before 31 December 2020, section 5(4) of the 2018 Act is disapplied and the provisions of the EU Charter therefore continue to apply in these proceedings.

34. A helpful summary of the approach to be adopted following the UK's departure from the EU can be found in the judgment of Green LJ in *Lipton v BA City Flyer Ltd* [2021] EWCA Civ 454; [2021] 1 WLR 2545, at paras. 52-70. In particular, at paras. 63-64, Green LJ referred to the "general principles of EU law", to which the EU Charter may continue to have relevance. It should be noted, however, that, in the present case, the Claimant is entitled to rely on the Charter directly and not simply indirectly via the general principles of EU law: this is because of the transitional provision in para. 39(3) of Sch. 8 to the 2018 Act.

35. Another helpful summary can be found in the judgment of Warby LJ in *R (Open Rights Group Ltd) v Secretary of State for the Home Department* [2021] EWCA Civ 1573; [2022] QB 166, at para. 23, in particular at sub-paras. (1) – (3):

> "(1) A UK court must now decide any question as to the validity, meaning or effect of any retained EU law for itself: it is no longer possible to refer any matter to the CJEU: EUWA, section 6(1)(b).
>
> (2) But the general rule is that the court must decide any such question in accordance with any retained case law and any retained general principles of EU law that are relevant: EUWA, section 6(3). 'Retained EU case law' and 'retained general principles' mean principles laid down and decisions made by the CJEU before IP completion day.
>
> (3) When it comes to principles laid down or decisions made by the CJEU after IP completion day, the court is not bound (EUWA, section 6(1)) but 'may have regard' to them (EUWA, section 6(2))."

36. Accordingly, the legal position is that, although the UK has left the EU, the e-Privacy Directive and the EU Charter remain relevant in these proceedings as part of retained EU law. Furthermore, those instruments have the effect given to them by the principle of the supremacy of EU law and take precedence even over primary legislation enacted by the Westminster Parliament. That this is so is simply the consequence of the will of Parliament itself, in enacting the 2018 Act in the terms in which it did. Furthermore, if and to the extent that Parliament is not content, it now has the freedom to legislate contrary to retained EU law, which it could not have done while the UK was still a member of the EU.

37. It is also common ground that this Court is still bound by retained EU case law, including the judgments of the CJEU in *Privacy International* and *La Quadrature*, since those judgments were handed down before the end of the implementation period (31 December 2020). Decisions of the CJEU which have been given after that date are not binding on this Court although we are entitled to take them into account.

The 2018 judgment

38. The background to the EU law aspects of this case was set out by this Court in the 2018 judgment, at paras. 11-19. We will use the same abbreviations as we did in that judgment. We will refer to the Data Retention and Investigatory Powers Act 2014 as "DRIPA". We will refer to the decision of the CJEU in *Digital Rights Ireland Ltd v Minister for Communications, Marine and National Resources (Irish Human Rights Commission intervening)* (Joined Cases C-293/12 and C-594/12) [2015] QB 127 as *Digital Rights*. We will refer to the joined cases C-203/15 and C-698/15 *Watson v Secretary of State for the Home Department* and *Tele2 Sverige AB v Post-och*

telestyrelsen (Case C-203/15) as *Watson CJEU*: [2017] QB 771. We will refer to the decision of the Court of Appeal in *Watson* after the reference from the CJEU as *Watson CA 2018*: [2018] QB 912.

39. At paras. 118-138 of the 2018 judgment, we rejected the Claimant's contention that Part 4 of the IPA provides for the "general and indiscriminate" retention of traffic and location data. We set out our reasons in full and those should be treated as if they were incorporated into this judgment. In summary, as we said at para. 137:

> "… The overall amount of data which is retained under Part 4 … will be the outcome of applying a statutory regime which requires the contents of each retention notice to be necessary and proportionate. …"

At para. 135, we said:

> "In the light of this analysis of the structure and content of Part 4 … 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."

40. In the present case, Mr Jaffey rightly does not question what we said in relation to Part 4 (although that may be the subject of any future appeal) but he does submit that the reasoning set out there cannot be read over into consideration of Parts 5, 6 and 7 of the IPA. We will return to this submission later.

EU case law since the 2018 judgment

Privacy International

41. *Privacy International* did not concern the IPA but was concerned with earlier legislation, in particular section 94 of the Telecommunications Act 1984. Section 94, so far as material, provided:

> "(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the Government of a country or territory outside the United Kingdom.
>
> …

> (2A) The Secretary of State shall not give a direction under subsection (1) … unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct. …"

42. At the beginning of 2015 the existence of practices for the acquisition and use of bulk communications data by the security and intelligence agencies of the UK was made public, including in a report by the Intelligence and Security Committee of Parliament. In June 2015 Privacy International brought a complaint before the IPT challenging the lawfulness of those practices. As we have mentioned, in 2017 the IPT made a reference in that case to the CJEU. After setting out recitals as to the background circumstances, the IPT referred the following two questions to the CJEU:

> "(1) Having regard to Article 4 TEU and Article 1(3) of [Directive 2002/58], does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the [security and intelligence agencies] of a Member State fall within the scope of Union law and of [Directive 2002/58]?
>
> (2) If the answer to Question (1) is 'yes', do any of the [requirements applicable to retained communications data, set out in paragraphs 119 to 125 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970)] or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the [security and intelligence agencies] to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?"

43. In addressing the first question, at para. 44, the Court stated that "the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law …".

44. The Court answered the first question in the following way, at para. 49:

> "… Article 1(3), Article 3 and Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security

> and intelligence services for the purpose of safeguarding national security falls within the scope of that directive."

45. The Court answered the second question in the following terms, in the *dispositif*:

> "Article 15(1) of the e-Privacy Directive, read in the light of Article 4(2) TEU and Articles 7, 8, 11 and 52(1) of the Charter, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security."

46. When the *Privacy International* case returned to the IPT, the Tribunal (comprising Singh LJ, President, Edis LJ and Lieven J) gave judgment on 22 July 2021: [2021] UKIPTrib IPT_15_110_CH. The IPT granted a declaration that section 94 of the 1984 Act was incompatible with EU law. This was in substance the agreed position of the parties by that stage. The reasons for that incompatibility were set out in the judgment of the IPT, at paras. 19-21, with the three important caveats summarised at paras. 22-24. Those reasons were, first, that the only pre-conditions set down in the legislation for the making of a direction under section 94 were that:

(1) the Secretary of State had to consult the providers concerned;

(2) the directions appeared to the Secretary of State to be necessary in the interests of national security or relations with the Government of a country or territory outside the UK; and

(3) the Secretary of State believed the conduct directed to be proportionate to what was sought to be achieved.

Secondly, the legislative scheme did not provide for any limit to the duration of any direction. Thirdly, the legislative scheme did not require that any direction should be subject to review by a court or an independent administrative authority whose decision was binding.

47. As was made clear at para. 29 of its judgment, the IPT has not yet decided what the consequences of the declaration will be. That remains a matter of dispute between the parties and will be considered at a later stage, when the more general issue of remedies in that case is considered by the IPT.

La Quadrature

48. The joined cases in *La Quadrature* were the subject of a single judgment by the Grand Chamber of the CJEU, given on the same date as that in *Privacy International*.

So far as material, *La Quadrature* concerned the compatibility of French legislation (the Internal Security Code or "CSI") with EU law.

49. At para. 104, the CJEU concluded that national legislation which requires providers of electronic communication services to retain traffic and location data for the purposes of protecting national security and combatting crime falls within the scope of the e-Privacy Directive.

50. At para. 139, the Court said:

> "In view of the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter resulting from a measure involving the general and indiscriminate retention of data, it must be ensured that recourse to such a measure is in fact limited to situations in which there is a serious threat to national security as referred to in paragraphs 135 and 136 of the present judgment. For that purpose, it is essential that decisions giving an instruction to providers of electronic communications services to carry out such data retention be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed."

51. It is clear from the *dispositif*, in particular para. 1, that the Grand Chamber did not regard the e-Privacy Directive read in the light of the EU Charter, as precluding all legislative measures that may be described as involving "general and indiscriminate" retention of traffic and location data. Indeed, the *dispositif* identifies some circumstances in which such retention is permissible subject to certain safeguards.

The judgment of the Grand Chamber of the ECtHR in *Big Brother Watch*

52. The applications in *Big Brother Watch* and the related cases were brought before the 2016 Act and therefore concerned the regime in earlier legislation. In particular they concerned the legal framework for bulk interception which was then contained in section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA"). This permitted the Secretary of State to issue warrants for the interception of "external communications" and, pursuant to section 16 of RIPA, intercepted material could not be selected to be read, looked at or listened to "according to a factor which is referable to an individual who is known to be for the time being in the British Islands". It is important to note that many of the safeguards which are contained in the 2016 Act, and to which this Court referred in the 2019 judgment, were not present in the regime in RIPA: for example, there was at that time no requirement of the "double lock", involving a Judicial Commissioner. As we set out in more detail in the 2019 judgment, the Office of the Investigatory Powers Commissioner ("IPC") was created by the 2016 Act, although it replaced a number of earlier Commissioners.

53. At para. 424 of its judgment, the ECtHR accepted that "bulk interception is of vital importance to Contracting States in identifying threats to their national security". This had been recognised by the Venice Commission and by various Governments in the Council of Europe. It was also the conclusion of the Independent Reviewer of Terrorism Legislation (Lord Anderson of Ipswich QC) who, having examined a great deal of closed material, concluded that bulk interception was "an essential capability". He concluded that no alternative would be sufficient to substitute for the bulk interception power. Nonetheless, as the ECtHR continued at para. 425, there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for their private life. In a state governed by the rule of law, the ECtHR concluded that the section 8(4) regime, despite its safeguards, including some robust ones, did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it identified the following fundamental deficiencies in that 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. In consequence, at para. 426, the ECtHR found that section 8(4) did not meet the "quality of law" requirement in Article 8 and was therefore incapable of keeping the interference with such rights to what was necessary in a democratic society. For that reason the ECtHR found a violation of Article 8 of the Convention at para. 427.

54. The ECtHR also found an incompatibility with Articles 8 and 10 of the ECHR in relation to confidential journalistic material: see paras. 456-458 of the judgment. The ECtHR found that protections for journalists and confidential journalistic material (including journalistic sources) were insufficient. It held that selection by an intelligence agency of such material for examination or retention should be subject to prior independent approval.

55. The Government of the UK has accepted those parts of the judgment and proposes to amend the domestic legislative regime to remedy those defects. This was made clear in a written Ministerial Statement by the Home Secretary (Priti Patel MP) and the relevant Minister in the House of Lords (Baroness Williams of Trafford) on 31 March 2022: see para. 45 in the witness statement of Lucy Montgomery-Pott.

Grounds of challenge relating to Parts 3 and 4 of the IPA

The relationship between Parts 3 and 4 of the IPA

56. Part 4 of the IPA enables the Secretary of State to serve a notice (under section 87) on a telecommunications operator to retain "relevant communications data" for specified purposes, which include the interests of national security, the prevention or detection of crime and the economic well-being of the UK so far as relevant to national security. A retention notice may not be given without the approval of a Judicial Commissioner.

57. "Relevant communications data" does not include any "content" of a communication (section 261(5)). But it does include data to identify the sender or recipient of a communication, time and duration, method of communication, the transmission

system involved and its location (section 87(11)). A retention notice may relate, among other things, to a particular operator or a description of operators and it may require the retention of all data or any description of data (section 87(2)). Accordingly, the notice may require the retention of data in bulk. However, it may not require data to be retained for more than 12 months (section 87(3)).

58. Part 4 deals only with *retention* of relevant data. It does not authorise a security or intelligence service or other public authority to acquire or gain access to such data.

59. Part 3 of the IPA provides for the authorisation of the acquisition of communications data. An authorisation of this kind may be sought in relation to data retained by a telecommunications operator pursuant to a notice given under Part 4.

60. As with Part 4, an authorisation under Part 3 cannot relate to the content of a communication.

61. There are three different powers to grant authorisations under Part 3. Section 84 applies those powers to postal operators with modifications.

62. The first power, contained in section 60A, was inserted into the IPA by the 2018 Regulations as part of the response to the declaration made by this Court in the 2018 judgment. The Court had decided that access to retained data had to be subject to prior review by a court or by an independent administrative body in cases not involving national security (applying *Watson CJEU* and *Watson CA 2018*).

63. Section 60A enables a "relevant public authority" (as shown in the Table in Sch. 4 – see section 70(2)), and in some instances a local authority (see section 73), to apply to the IPC for an authorisation essentially to obtain communications data relating to a telecommunications system. The IPC has delegated this function to the Office for Communications Data Authorisations ("OCDA") to act on his behalf. The IPC must be satisfied that the acquisition of data is necessary for a purpose in section 60A(7) which provides:

> "It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—
>
> (a) in the interests of national security,
>
> (b) for the applicable crime purpose (see subsection (8)),
>
> (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
>
> (d) in the interests of public safety,
>
> (e) 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,

> (f) to assist investigations into alleged miscarriages of justice, or
>
> (g) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
>
> (i) to assist in identifying P, or
>
> (ii) to obtain information about P's next of kin or other persons connected with P or about the reasons for P's death or condition."

64. In section 60A(8) the "applicable crime purpose" refers to the prevention or detection of "serious crime" where the communications data is wholly or partly "events data" (as defined in section 261(4)), and the prevention or detection of "crime", or the prevention of disorder, in the case of other communications data. The definition of "serious crime" in section 263(1) is extended by section 86(2A) for the purposes of Part 3 of the IPA. Although in its skeleton argument, the Claimant had contended that this definition of "serious crime" was too wide to be compatible with EU law, Mr. Jaffey rightly chose not to pursue this in oral submissions and we say no more about it.

65. In addition, the IPC must be satisfied that it is necessary for the authority to obtain the communications data for the purposes of a specific investigation or operation or for testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of such data. The IPC must also be satisfied that the conduct to be authorised is proportionate to what is sought to be achieved (section 60A(1)(b) and (c)).

66. The second power, contained in section 61 (as amended by the 2018 Regulations), enables a "designated senior officer" of a "relevant public authority" to grant an authorisation to any officer of that authority to obtain communications data from any person which relates to a telecommunications system or data derived from such a system (section 61(2)). The designated senior officer must be satisfied that it is necessary to obtain that data for a purpose falling within section 61(7), for a specific investigation or operation, or for testing, maintaining or developing equipment or capabilities relating to communications data and that the conduct authorised would be proportionate to what is sought to be achieved (section 61(1) and (2)).

67. The 2018 Regulations amended section 61(7) so that the only purposes for which the obtaining of data may be authorised under section 61 are restricted to:

(1) the interests of national security; or

(2) "the applicable crime purpose" (defined in section 61(7A) in the same terms as section 60A(8)); or

(3) the interests of the economic well-being of the UK so far as relevant to the interests of national security.

68. So, if an authority wishes to obtain communications data for the broader purposes set out in section 60A(7), that is in the interests of public safety, to prevent death, or to prevent or mitigate injury or damage to a person's physical or mental health, or to assist in investigating an alleged miscarriage of justice, or to assist in identifying a deceased person or person who cannot identify themselves because of a physical or mental condition, authorisation has to be sought from the IPC under section 60A.

69. The power of internal authorisation under section 61 is also subject to the restrictions in sections 70 and 73 and Sch. 4. The 2018 Regulations inserted subsection (5A) into section 70 and amended the Table in Sch. 4 so that a relevant authority which is a police force may only seek an authorisation under section 61 in the interests of national security or the economic well-being of the UK so far as relevant to national security. Such an authority may not seek an internal authorisation for the "applicable crime purpose". Only a security or intelligence service may seek to rely upon section 61 for that purpose; they may do so as a freestanding purpose, that is, even if the authorisation is not also necessary for reasons of national security or the economic well-being of the UK related to national security. This distinction is the subject of one of the grounds of challenge brought by the Claimant.

70. Thirdly, section 61A of the IPA was added by the 2018 Regulations to enable a designated senior officer to grant an internal authorisation in urgent cases. By virtue of section 70(6) and the Table in Sch. 4, the range of purposes for which such an urgent authorisation may be sought is generally broader. For example, a police force may obtain a section 61A authorisation where there is an urgent need to obtain communications data for "the applicable crime purpose". However, the Claimant takes no point on the compatibility of section 61A with retained EU law.

71. Sections 62 to 66 impose further restrictions on the authorisations which may be granted under Part 3. Under section 62 local authorities may not acquire internet connection records for any purpose and the ability of other public authorities to access such records is restricted to specific circumstances and purposes. Subject to certain exceptional circumstances, a designated senior officer may not grant an authorisation under section 61 for the purposes of a specific investigation or operation on which he or she is working (section 63). Section 65 restricts the duration of an authorisation under section 60A or section 61 to one month, and under section 61A to three days, subject to renewal or cancellation. Section 66 imposes a duty on a telecommunications operator upon whom a requirement is imposed by virtue of an authorisation under Part 3, to obtain or disclose the relevant data in a way that minimises the amount of data that needs to be processed for the relevant purpose.

72. In *Watson CJEU* the Court decided that the e-Privacy Directive applies to legislation which requires a provider of electronic communications services to retain "traffic and location data" (or "communications data" under the IPA), since to do so necessarily involves the provider in "processing" that data for the purposes of article 3(1) (para. 75). Furthermore, legislation which, by Article 15(1) of the Directive, requires a provider to grant a public authority access to retained data, also involves the processing of that data by that provider. Accordingly, such access to retained data also falls within the ambit of the Directive (paras. 76 and 78). There was no dispute

between the parties that, for the purposes of the hearing before us, the e-Privacy Directive does apply, to this extent, to the powers under Parts 3 and 4 of the IPA to require communications data to be retained and to obtain access to that data.

Notification to persons whose data has been accessed

73. The Claimant submits that a relevant public authority is required by EU law to give notice of having accessed data under Part 3 of the IPA as soon as operationally possible to the persons affected by that access. The Claimant relies upon the decision in *Watson CJEU*, at para. 121, where the Court stated:

> "Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95)."

However, we note that this conclusion did not form part of the Court's *dispositif.*

74. Article 15(2) applied chapter III of the Data Protection Directive (95/46/EC) to national legislation giving effect to the e-Privacy Directive and to the individual rights it creates. Article 22 of Directive 95/46/EC required that every person should have the right to a judicial remedy for any breach of the rights guaranteed by the national law in relation to the processing in question.

75. The reference in *Watson CJEU* to C-362/14 *Schrems v Data Protection Commissioner* [2016] QB 527 relates to a part of that decision which was concerned with a lack of judicial remedy, not with the issue of whether access to data must be notified to persons affected to enable an existing legal remedy to be exercised. C-553/07 *College van burgemeester en wethouders van Rotterdam v Rijkeboer* [2009] 3 CMLR 28 was also concerned with a different matter, namely a citizen's right of access under article 12 of Directive 95/46/EC to information about data relating to him. In any event, article 13 authorised derogations from, among others, article 12 to safeguard certain public interests, such as national security and the investigation of criminal offences. Accordingly, we do not consider that these decisions provide any material support for the CJEU's statement in *Watson CJEU* at para. 121.

76. In *Watson CA 2018* the Court of Appeal refused to make a declaration that, by virtue of *Watson CJEU* at para. 121, DRIPA and RIPA infringed EU law by failing to provide for notification. The Court also refused to refer the issue to the CJEU,

because it was clear that the matter would be before the CJEU when it considered the reference by the IPT in *Privacy International*.

77. In the 2018 judgment this Court dealt with the notification issue at paras. 173-183. The Court refused to make a further reference of this issue to the CJEU, and stayed this part of the claim pending the decision of the CJEU in the *Privacy International* case. However, as things have turned out, the CJEU did not address the notification issue in its decision in *Privacy International.*

78. Both parties referred us to paras. 190-191 of the CJEU's decision in *La Quadrature*. In our judgment, it is clear from paras. 183-189 and from para. 190 that the context for the Court's observations at paras. 190-191 was the "real-time" collection of traffic and location data in respect of an individual identified as having links to a terrorist threat. The authorisation allowed the authorities to monitor for its duration, continuously and in real-time, the person with whom the subject was communicating, places of residence, movements and location of equipment used. The CJEU considered this data to be particularly sensitive, so that real-time access to such data had to be distinguished from non-real time access. The former allowed monitoring that was "virtually total" (para. 187).

79. It was in that context that the CJEU stated that a national authority carrying out real-time collection of traffic and location data must notify the persons concerned, to the extent that, and as soon as, notification is no longer liable to jeopardise the tasks for which the authority is responsible (para. 190). The CJEU also indicated, at para. 191, that, where an individual is identified following automated analysis, notification to that person may become necessary, subject to those tasks not being jeopardised. We doubt whether it is proper to read across those brief statements in paras. 190 and 191, made by the CJEU in the context we have described, to Part 3 of the IPA. In any event, the issue of notification needs to be considered more broadly.

80. In our judgment, it is also necessary to read para. 121 of *Watson CJEU* in context. The paragraph begins with the word "likewise", confirming its close link with para. 120. There the CJEU had laid down the requirement that, save in cases of urgency, access by a public authority to retained data should generally be subject to prior review by either a court or an independent administrative body responding to a reasoned application by that authority. The CJEU itself drew an analogy with Article 8 of the ECHR and one of the leading cases decided under the Convention, *Szabo and Vissy v Hungary* (2016) 63 EHRR 3. We accept the submission of Sir James Eadie that in this context it is relevant to have regard to jurisprudence of the ECtHR.

81. We refer to the extensive and helpful discussion of the notification issue by the ECtHR in *Big Brother Watch* at paras. 335-337, 350, 357-361 and 413-415. In summary, the ECtHR held that, in deciding whether legislation breaches Article 8 of the ECHR, the court may have regard to *any* notification mechanisms and the remedies provided by national law (para. 335). Notification is described as a "relevant factor" in assessing the effectiveness of remedies before the court and hence the existence of effective safeguards against the abuse of surveillance powers (para. 337). The ECtHR went on to state:

> "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the

> measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Z*akharov, cited above, § 234; see also *Kennedy*, cited above, § 167)."

82. Thus, the ECtHR has plainly decided that there is no absolute requirement for notification. It suffices that a person who suspects that he or she has been subject to surveillance can apply to a court the jurisdiction of which does not depend on notification having been given to that person of the measures taken. We note that in *Kennedy v the United Kingdom* (2011) 52 EHRR 4, the ECtHR highlighted the extensive jurisdiction of the IPT to examine any complaint, in that instance of unlawful interception. This included the ability of any person who suspects that his communications have been intercepted to apply to the Tribunal, "unlike many other domestic systems" (*Kennedy* at (para. 167)). In *Big Brother Watch* the court reiterated that view at para. 357 and added that a remedy which does not depend upon notification may in some circumstances offer better guarantees of a proper procedure (para. 358).

83. At para. 359 the ECtHR accepted that an effective remedy could be given by a non-judicial body provided that it is independent, adopts a fair procedure and reaches a reasoned, legally binding conclusion. The IPT fulfils those requirements. It is also a judicial body and, since the end of 2018, its decisions may be the subject of an appeal.

84. At paras. 413-414 of *Big Brother Watch* the ECtHR summarised the broad powers and procedures of the IPT. It decided that the Tribunal "provides an effective remedy for applicants complaining both of specific incidences of surveillance and the general Convention compliance of surveillance regimes", through a jurisdiction which does not depend upon notification of interception to the subject. The Grand Chamber's overall conclusion was that "the IPT provided a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services" (para. 415).

85. We find the reasoning of the ECtHR on effective remedy without notification of access having taken place to be compelling. That court considered the arrangements under RIPA. We agree with Sir James Eadie that their conclusions apply *a fortiori* to the IPA. It is also significant that in *Watson CJEU* and in *Privacy International* the CJEU considered section 94 of the Telecommunications Act 1984. That court has not considered the extensive code in the IPA; nor the extensive jurisdiction of the IPT; nor, it would appear, any comparable code.

86. Our conclusion is reinforced by the procedures for reporting serious errors to persons affected.

87. The Communications Data: Code of Practice was issued under Sch. 7 to the IPA in November 2018. A person exercising any function under the legislation must have regard to that code and a court or tribunal may take into account a failure to do so (para.6 of Sch. 7). Where communications data is wrongly acquired or disclosed, the public authority which made the error, or established that the error has been made, must report that fact to the authority's senior responsible officer and to the IPC (paras. 14.4 to 14.6 of the Code).

88. Under section 231 the IPC must inform a person concerned of any error by a public authority in complying with any requirements under the IPA (or other legislation) which are subject to review by the IPC, or any error of a kind described in a code, where the IPC consider that error to be "serious" and disclosure to be in the public interest (section 231(1) to (4) and (9)). When the IPC informs a person of such an error, he must also inform them of any rights they may have to apply to the IPT and provide such details as he considers necessary for the exercise of those rights (section 231(6)). We note that the annual report of IPCO for 2020 provides a practical example of the notification of a serious error to a person who had wrongly been thought to be connected with a crime under investigation: see the witness statement of Lucy Montgomery-Pott, at para. 27.

89. We have reached the firm conclusion that Parts 3 and 4 of the IPA comply with the requirement in Article 15(2) of the e-Privacy Directive for a citizen to have a right to a judicial remedy to address breaches of the legislation, and in particular an effective judicial remedy. This is secured by the jurisdiction of the IPT, section 231 of the IPA and the Code of Practice. EU law does not require the exercise of the powers under Part 3 to authorise access to communications data retained under Part 4 to be subject to any additional obligation of notification to persons affected by such access. Accordingly, this ground of challenge must be rejected.

Retention of Data within the EU/UK

90. The Claimant relies upon *Watson CJEU* at paras. 122 and 125 for the proposition that data accessed under Part 3 must be retained within the EU/UK:

> "[122] With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make

> provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the *Digital Rights Ireland* case [2016] QB 127, paras 66-68).
>
> …
>
> [125] Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."

91. Mr. Jaffey submitted that, although those passages are directed to the retention of data by service providers, once such data is acquired by a public authority under Part 3 of the IPA, the same concern arises: it might be transferred outside the UK or the EU to a place where the safeguards required by EU law do not exist.

92. It follows from *La Quadrature* at para. 134 that the statement in *Watson CJEU* at para. 122 cannot be taken as applying to the exercise of powers under Parts 3 and 4 of the IPA for national security purposes.

93. The *Digital Rights* case, cited in *Watson CJEU* at para. 122, was concerned with the blanket provisions for retention of data in Directive 2006/24/EC which the CJEU held to be invalid. At para. 68 the CJEU criticised the failure of the Directive to require the data in question to be retained in the EU so that the controls by an independent authority required under paras. 66-67 could be ensured. Those were controls for protecting the integrity and confidentiality of the data, access to that data and its destruction. Although the court referred at para. 68 to Case C-614/10 *Commission v Austria* it would appear that *Digital Rights* was the first decision in which the CJEU indicated that data should remain within the EU and that this was justified by the need to ensure that protections afforded by EU law could continue to be applied.

94. *Watson CJEU* was considered by the Court of Appeal in *Watson CA 2018.* The Court dealt with retention of data in the EU at paras. 14-19. It referred to considerable uncertainty about the meaning and effect of para. 122 in *Watson CJEU,* including whether it purported to lay down an absolute requirement. In addition, the IPT had included a question about this requirement in its a reference to the CJEU in *Privacy International*. The IPT was concerned, among other things, that it conflicted with Article 25 of the then Data Protection Directive (Directive 95/46/EC) providing for

the free movement and transfer of data to third countries. The Court of Appeal expressed the hope that such uncertainties would be addressed by the CJEU and the law clarified when it considered the reference by the IPT. In the circumstances, the Court of Appeal refused to make any declaration on the issue (para. 19).

95. The CJEU analysed the scheme of the former Directive 95/46/EC in *Schrems* at paras. 46-60. Article 25(1) of the Directive allowed a transfer of personal data to be made to a third country if that country would ensure an "adequate level of protection". Article 25(2) provided, in summary, for that adequacy to be assessed in the light of all the surrounding circumstances, the nature of the data, the duration of the processing operation, the rules of law in force in the third country and the security measures applied there. Article 31(6) enabled the Commission to issue a decision, with which Member States would then comply, that a third country would ensure an adequate level of protection within the meaning of Article 25(2). The straightforward point is that, if data protection legislation allows for the transfer of data to third countries subject to the legal systems of those countries ensuring adequate safeguards for the protection of that data, why should para. 122 of *Watson CJEU* be treated as an absolute requirement? Indeed, why is that requirement needed at all?

96. In the 2018 judgment this Court addressed the retention of data within the EU at paras. 163-172. At para. 164 the Court recorded Mr. Jaffey's statement that the Claimant was no longer contending that any such requirement should be treated as absolute. The Court went on to explain that the issues relating to whether there is a requirement for data to be retained in the EU and, if so, the nature of that requirement, were fairly and squarely raised by the reference to the CJEU already made by the IPT in *Privacy International*. Accordingly, this Court refused to order a further reference and stayed this part of the claim for judicial review pending the CJEU's decision in *Privacy International*.

97. It is common ground before us that the CJEU did not address that issue in its decision in *Privacy International* or in *La Quadrature*. Despite the conflict identified with the Directive 95/46/EC and, by parity of reasoning, with its replacement in Chapter V of Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR") (see e.g. regulation 45), the CJEU has not returned to the subject. By the same token, it may be noted that the CJEU has not reaffirmed para. 122 of *Watson CJEU*.

98. The Claimant's case has not attempted to address this conflict between *Watson CJEU* at para. 122 and EU law on data protection and transfer. The Defendants submit that para. 122 of *Watson CJEU* must be read harmoniously with other EU legislation on data protection and, in particular, as being subject to the principles on transfer of data out of the EU, notably in the GDPR. We accept those submissions.

99. The UK gave effect to the GDPR when it enacted the Data Protection Act 2018 ("DPA"). That statute has since been amended to address Brexit, in particular, by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019 No. 419). The DPA, as amended, applies alongside the "UKGDPR", the UK's "retained EU law" version of the 2016 EU Regulation.

100. Transfers of data outside the UK by the security and intelligence services are permitted by section 109(2) of the DPA.

101. Law enforcement processing is dealt with in Part 3 of the DPA. Chapter 5 deals with the transfer of personal data to third countries or international organisations. In general, such transfers must either accord with regulations which treat a third country as providing an adequate level of protection for personal data (including an independent authority in the third country to ensure and enforce compliance with data protection rules), or be subject to a binding legal instrument providing appropriate safeguards. In Part 3 a "third country" refers to a country outside the UK (section 33(7)). For completeness, we also mention Chapter 2 of Part 2, which provides for regulations to ensure adequate protection and safeguards where personal data in other fields is to be transferred to a third country.

102. On 28 June 2021 the European Commission announced that it had issued two "adequacy decisions" concerning the UK after its departure from the EU, one under the EU's GDPR and the other under the Law Enforcement Directive (Directive (EU) 2016/680). The Commission stated that the decisions allowed data to flow freely from the EU to the UK, "where it benefits from an essentially equivalent level of protection to that guaranteed under EU law". The Commission also stated that "the UK has fully incorporated the principles, rights and obligations of the GDPR and the Law Enforcement Directive into its post-Brexit legal system". The Commission added that the adequacy decisions facilitate the correct implementation of the EU-UK Trade and Co-Operation Agreement.

103. From all these materials it is apparent that the objective in para. 122 of *Watson CJEU*, of ensuring that EU law safeguards continue to apply to any accessed data transferred outside the EU, is satisfied by the UK's domestic data protection law, which is acknowledged by the EU to satisfy the requirements of EU law. Mr Jaffey made no submission to the contrary.

104. We therefore conclude that UK rules on the transfer to a third country (including a country outside the EU) of data falling within Parts 3 and 4 of the IPA do not breach any principle of EU law. Accordingly, this ground of challenge must be rejected.

Do Parts 3 and 4 meet EU law requirements in relation to automated processing of data?

105. The Claimant's case on this issue was based upon paras. 172-182 of *La Quadrature*.

106. That part of the CJEU's decision was concerned with French legislation which enabled a state authority to direct a provider of electronic communications services to screen all its retained traffic and location data, by using parameters given by the authority for automated analysis (para. 172). The CJEU held that such an exercise carried out by a provider amounted to "general and indiscriminate processing" on behalf of the authority. They also treated that processing as being independent of the subsequent decision by the French Prime Minister to authorise the identification of a person from the results of that analysis as a potential terrorist threat and the collection of related data (paras. 43 and 172). Accordingly, the automated analysis had to be justified as a derogation under Article 15(1) of the e-Privacy Directive, satisfying the requirements for legal definition, necessity and proportionality (paras. 175-176).

107. The authorisation of automatic analysis of such a "general and indiscriminate" nature must ensure that certain safeguards will be observed (para. 179). For that type of data processing:

(i) pre-established models and criteria should be specific and reliable, making it possible to identify individuals who might reasonably be suspected of participating in terrorism (in that instance) (para. 180);

(ii) the models and criteria should be non-discriminatory, in the sense that they do not rely *in isolation* on sensitive data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or a person's health or sex life (paras. 180-181);

(iii) since automated analysis is subject to a margin of error, any positive result obtained must be subject to independent examination by "non-automated measures" before adopting a measure adversely affecting that person (para. 182); and

(iv) the models and criteria should be subject to regular re-examination to ensure that they are reliable and up to date (para. 182).

The Claimant's case that automated analysis under Part 3 of the IPA breaches EU law is based solely upon safeguard (ii), the avoidance of discrimination by not using sensitive data of the kinds listed "in isolation", as opposed to not using such data at all.

108. In the 2018 judgment this Court held, at paras. 118-138, that Part 4 does not provide for the general and indiscriminate retention of data. We reach the same conclusion in relation to Part 3 for a number of reasons.

109. First, before an officer in a relevant public authority makes an application under section 60A, or before a designated senior officer grants an application under section 61 or section 61A, the officer accredited within the authority to act as a "single point of contact" must be consulted about the proposal, so that he or she may advise, among other things, on any issues about the lawfulness of the proposed authorisation and the possibility of its having unintended consequences (section 76).

110. Secondly, the IPC's power to authorise access is restricted by the tests of necessity in relation to the purposes of section 60A(7) and proportionality. As we have explained, the powers in section 61 are limited to national security, save in the case of the intelligence and security services, where an internal authorisation may be obtained purely for the "applicable crime purpose", a subject to which we return below. Section 61A deals with cases of urgency, where the permissible purposes are slightly wider. But the necessity and proportionality tests apply to all authorisations made under sections 61 and 61A.

111. Thirdly, the IPC, and OCDA on his behalf, act as independent authorising bodies. Save in defined exceptional circumstances (such as an imminent threat to life or other emergency) a designated senior officer may not grant an authorisation for the purposes of a specific investigation or operation if he or she is working on that matter (section 63).

112. Fourthly, the powers in Part 3 to authorise access may only be used where it is necessary for the relevant public authority to obtain data for a specific investigation or operation or to test, maintain or develop equipment or systems. That is why Parliament has described these as "targeted" authorisations.

113. Fifthly, section 65 limits the duration of an authorisation under sections 60A or 61 to one month and under section 61A to three days.

114. Sixthly, by section 66 a telecommunications operator which obtains or discloses data in response to an authorisation is obliged to obtain or disclose the relevant data in a way which minimises the amount of data that needs to be processed.

115. Seventhly, if an officer of OCDA grants an authorisation under section 60A, or a designated senior officer grants an authorisation under section 61 or section 61A, for the purposes of identifying or confirming a source of "journalistic information" and the authorisation is not necessary because of an imminent threat to life, the authorisation does not have effect unless approved by a Judicial Commissioner (section 76(1) and (2)). Section 77(6) requires the IPC 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 seeks to identify or confirm a source of journalistic information.

116. Eighthly, OCDA or the officer considering whether to grant an authorisation under Part 3 must have regard to the factors listed in section 2(2) of the IPA, read with section 2(3)-(5). The effect of those provisions was summarised in the 2018 judgment at para. 133.

117. For these reasons the authorisations that may be granted under Part 3 are not to be treated as "general and indiscriminate" in the sense used in *La Quadrature.* We therefore doubt whether the observation by the CJEU at paras. 180-181 on "discrimination in isolation", in the context of legislation of a very different nature and effect, should be applied to the authorisation powers in Part 3 of the IPA.

118. However, even assuming that that observation is applicable to Part 3, we accept Sir James Eadie's submission that it does not call for a specific provision incorporating that language to be included in domestic legislation such as the IPA. The CJEU did not indicate that that degree of specificity is a requirement of EU law.

119. In any event, in our judgment the principle stated at paras. 180-181 of *La Quadrature* is adequately addressed by section 2(2) of the IPA and by the requirements in Part 3 for the authorising person to be satisfied that the proportionality test is satisfied. The non-discriminatory requirement identified by the CJEU is but one of a number of considerations which are relevant to those tests. There is no legal necessity for all such matters to be listed expressly in legislation (see also the 2018 judgment at para. 124).

120. Accordingly, in our judgment part 3 of the IPA does not breach paras. 180-181 of *La Quadrature.* For these reasons we reject this ground of challenge.

Do Parts 3 and 4 meet the requirement outside national security for prior independent authorisation?

121. The Claimant contends that there is one respect in which Part 3 of the IPA, as amended after the declaration made by this Court after the 2018 judgment, does not comply with the *Watson CJEU* requirement for prior independent authorisation of access to communications data. Under section 61 a security or intelligence service may obtain an internal authorisation from a designated senior officer to gain access to data for the "applicable crime purpose" and, in those circumstances does not need to make an application to the IPC under section 60A.

122. In *Watson CJEU* the court held that in the context of fighting serious crime, access to retained data should as a general rule, except in cases of validly established urgency, "be subject to a prior review carried out either by a court or by an independent administrative body" (para. 120). That requirement was also included in the *dispositif*. The security and intelligence services were able to exercise the powers examined by the CJEU.

123. In *Watson CA 2018* it was common ground that access to retained data for the prevention, investigation or detection of crime has to be limited to serious crime and is subject to prior review by a court or independent administrative body. In the 2018 judgment this Court made the same point at paras. 18 and 186; and in the declaration granted by the Court, which defined the incompatibility of Part 4 of the IPA with EU law.

124. In our judgment, an "independent administrative body" must refer to a body independent of the body applying for an authorisation. Accordingly, the expression does not embrace internal authorisation by one senior officer in response to an application made by another officer within the same organisation, even if independent of the investigation concerned. Sir James Eadie sought to rely upon *Big Brother Watch* at para. 355, where the ECtHR accepted that "prior internal authorisation" would be sufficient at the later stage when "strong selectors" linked to identifiable individuals are chosen by security and intelligence services for use in their analysis of the data they have obtained. But that passage was not addressing the question of whether prior authorisation to access retained data should be granted in the first place. It does not assist the Defendants to advance a legal justification for the different treatment of the security and intelligence services in relation to the "applicable crime purpose".

125. Sir James Eadie also sought to justify this difference by reference to certain practical considerations. With respect, we are unable to accept that submission. The points raised were not supported by any evidence and did not appear to us to provide any sound basis to justify the distinction for which the Defendants contend. The police can and do operate in the field of national security. They must distinguish between a national security purpose and ordinary criminal purposes when they apply the legislation, since self-authorisation is not permitted to them if they are acting for an ordinary criminal purpose.

126. Further, it is clear that the statutory purposes of the security and intelligence agencies include acting to prevent or detect crime, in other words for ordinary criminal purposes which may not be connected with national security.

127. Section 1 of the Security Service Act 1989 sets out the functions of the Security Service in the following terms, at subsections (2)-(4):

> "(2) The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
>
> (3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.
>
> (4) It shall also be the function of the Service to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime."

128. It will be apparent in particular from the words of subsection (4) that the functions of the Service are not confined to national security matters but can include supporting the activities of the police and other law enforcement agencies "in the prevention and detection of serious crime."

129. Section 1(2) of the Intelligence Services Act 1994 provides that the functions of the Secret Intelligence Service shall be exercisable only for certain purposes, which include, at para. (c) "in support of the prevention or detection of serious crime." Similarly, section 3(2)(c) sets out a similar function in relation to the Government Communications Headquarters ("GCHQ").

130. When the security and intelligence agencies act for an ordinary criminal purpose, we cannot see any logical or practical reason why they should not be subject to the same legal regime as the police. The mere fact that in general they operate in the field of national security cannot suffice for this purpose. It is the particular function in issue which is relevant. Moreover, the identity of the body carrying out a relevant function is immaterial: what is crucial is the function being carried out, not the identity of the body performing it.

131. In our judgment the law as stated by the CJEU, and by the Court of Appeal and the Divisional Court in this country, is clear. Prior authorisation by a court or independent administrative body is required for access under Part 3 to data retained under Part 4. The ability of the security and intelligence agencies to obtain access to retained data for the "applicable crime purpose" by relying upon section 61 rather than section 60A is incompatible with retained EU law.

132. The Claimant succeeds on this particular ground of challenge, but the other grounds of challenge to Parts 3 and 4 of the IPA are rejected.

The argument based on Big Brother Watch

133. The Claimant's grounds of challenge to Parts 3 and 4 of the IPA include an argument based on the judgment of the ECtHR in *Big Brother Watch*, which is identical to the argument it makes in that respect in its challenge to Parts 5, 6 and 7. We will therefore deal with it when we address it in that context below.

Grounds of challenge in relation to bulk powers in Parts 5, 6 and 7 of the IPA

134. This part of the Claimant's challenge relates to the following "bulk" powers. First, in Part 6 of the IPA: the power to issue bulk interception warrants in chapter 1; the power to issue bulk acquisition warrants in chapter 2; and the power to issue bulk equipment interference warrants in chapter 3. The Claimant also challenges the power to issue thematic equipment interference warrants in Part 5, insofar as it applies other than to a single person or premises. Finally, the Claimant challenges the power to retain bulk personal datasets under Part 7 of the IPA, read with the relevant powers of the security and intelligence agencies to obtain, retain and use data.

135. The Defendants contest the proposition that Part 7 falls within the scope of EU law at all. This is because the retention of bulk personal datasets has nothing to do with communications services providers ("CSPs", in other words third parties, but only concerns actions of state authorities: the security and intelligence agencies.

136. In outline, the Claimant submits that the bulk provisions are incompatible with EU law for the following four reasons:

(1) The scope of the bulk provisions is too broad. It is submitted that they allow "general and indiscriminate" retention (including obtaining) and access regimes, but the purpose of retention and access to data is not limited to national security.

(2) In the national security context (and outside it), the bulk provisions do not meet the EU law requirements as to automated processing of data, including non-discrimination.

(3) Outside the national security context, the safeguards identified by the CJEU in *Watson* are absent, namely: prior independent authorisation of access; notification to the subject where operationally possible; and retention of data within the UK or EU.

(4) The bulk provisions do not comply with the requirements of Articles 8 and 10 of the ECHR, in particular concerning journalistic and lawyer-client communications, and for that reason are also not compatible with EU law.

At the hearing before us Mr Jaffey did not make submissions in relation to lawyer-client communications but did maintain his submission in relation to journalistic ones.

137. As we have mentioned above, the Claimant also makes the same argument in relation to the ECHR when challenging Parts 3 and 4 of the IPA.

138. We do not accept the submissions for the Claimant. We will address the arguments based directly on EU law first and will then turn to the argument based on the judgment of the ECtHR in *Big Brother Watch*.

EU law

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 CSPs 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 CSPs, 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.

140. Secondly, we do not accept the Claimant's submission that the bulk powers provisions in the IPA are "general and indiscriminate" as that term is used by the CJEU. The Claimant in effect conflates bulk provisions with general and indiscriminate ones. We accept the Defendants' submission that this Court's earlier analysis of Part 4 of the IPA is applicable to the other Parts of the Act which provide for bulk powers: see the 2018 judgment, at paras. 118-138.

141. Thirdly, this Court has already held, in the 2019 judgment, that the bulk powers provisions of the IPA are compatible with the ECHR. The reasons which we gave for that conclusion are in substance the same as would be required under EU law. The main points can be summarised as follows:

(1) None of the bulk powers imposes a blanket requirement of retention. There must be an application by the head of an intelligence service, or a person acting on their behalf, to the Secretary of State for a warrant issued in accordance with the relevant Part of the Act.

(2) Each of the powers requires the Secretary of State to be satisfied as to the necessity and proportionality of the warrant for one or more of the specified statutory purposes.

(3) Each of the bulk powers is subject to approval by a Judicial Commissioner.

(4) The safeguards against the risk of abuse of the bulk powers also include the role played by the Office of the IPC and the jurisdiction of the IPT.

142. As we said in the 2019 judgment, the IPA regime for bulk powers needs to be read as a whole. When that is done, it is clear that Parliament has provided a suite of inter-locking provisions, the cumulative effect of which is to render the legislation compatible with the requirements of the ECHR. The EU law requirements to prevent the risk of abuse of discretionary powers is in substance also complied with for the

same reasons. The requirements in *La Quadrature*, at para. 132, are materially similar to the requirements of the ECHR, which we have already addressed in the 2019 judgment.

Automated processing of data

143. We reject this part of the challenge for the reasons set out in paras. 105-120 above.

Prior independent authorisation of access

144. The Claimant complains that the bulk powers in the IPA fail to require independent authorisation for access to retained data each time data is accessed for a purpose falling outside national security, save where a targeted examination warrant is required under section 15(3) (and see also section 152(4)). It is submitted that the IPA does not accord with *Watson CJEU* at para. 120 in this respect.

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.

146. We therefore reject this part of the challenge.

Notification to persons whose data has been accessed

147. We reject this part of the challenge for the reasons set out in paras. 73-89 above.

Retention of data within the EU/UK

148. We reject this part of the challenge for the reasons set out in paras. 90-104 above.

The argument based on Big Brother Watch

149. As we have mentioned, the Defendants accept that, in the light of the judgment of the Grand Chamber in *Big Brother Watch*, the IPA must now be understood to be incompatible with the ECHR in two specific respects:

(1) Prior internal authorisation is required for the use of "strong selectors linked to identifiable individuals" to select material for examination from bulk intercept acquired under Chapter 1 of Part 6.

(2) The regime for bulk interception in Chapter 1 of Part 6 is incompatible with Article 10 of the ECHR, insofar as it does not require authorisation by a judge or other independent body, where (i) the intention of the search is to select confidential journalistic material for examination, or the selectors/search terms used are such as to make the selection of such material highly probable; or (ii) a decision is made to retain such material which has been inadvertently selected for examination.

150. The Claimant relies upon those concessions, and upon the judgment of the ECtHR, in the present proceedings under EU law. Mr Jaffey submits that the relevant rights in the EU Charter are at least as broad in their effect as in the ECHR. Accordingly, the authoritative determination of the Grand Chamber in *Big Brother Watch* must now be applied, via the route of EU law, so as to render the relevant provisions of the IPA unlawful under EU law. We reject that submission.

151. First, the judgment of the Grand Chamber in *Big Brother Watch* is not directly binding on this Court. This Court has a duty to take it into account where relevant, under section 2 of the HRA. We have already given our judgment on the compatibility of the IPA with the ECHR in the 2019 judgment, which is now under appeal to the Court of Appeal. What view the Court of Appeal will take is not a matter for us.

152. Secondly, we do not consider that the CJEU would regard itself as being bound by the judgment of the Grand Chamber in *Big Brother Watch*, although no doubt it would pay it great respect. This is because the CJEU jealously guards its own independence in relation to matters of EU law, even where there are corresponding rights in the ECHR.

153. At the hearing before this Court Mr Jaffey relied upon a passage in the judgment of the CJEU (Third Chamber) in Case C-400/10 PPU *McB v LE* [2011] Fam 364. At para. 53, the Court said:

> "… It follows from Article 52(3) of the Charter that, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, their meaning and scope are to be the same as those laid down by the ECHR. However, that provision does not preclude the grant of wider protection by European Union law. … The wording of Article 8(1) of the ECHR is identical to that of … Article 7 [of the Charter], except that it uses the expression 'correspondence' instead of 'communications'. That being so, it is clear that … Article 7 contains rights corresponding to those guaranteed by Article 8(1) of the ECHR. Article 7 of the Charter must therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the caselaw of the European Court of Human Rights …"

154. We do not accept that that passage can bear the weight which Mr Jaffey sought to place upon it. We do not read that passage as being inconsistent with the longstanding jurisprudence of the CJEU to the effect that, while it is desirable for there to be a consistent interpretation of equivalent provisions in the Charter and the ECHR, ultimately the institutions of the EU, in particular the CJEU, are autonomous and do not regard themselves as being bound by judgments of the ECtHR.

155. It was for this reason, amongst others, that the CJEU (Full Court) said in its *Opinion 2/13 on accession to the ECHR by the EU* that it would not be possible for the EU to become a party to the ECHR on the terms then proposed: see paras. 155-200. Although in principle the Treaty on European Union, Article 6(2), envisaged the possibility that the EU could accede to the ECHR, this had to be done in a way which is compatible with the nature of EU law. The CJEU reiterated fundamental principles as to the unique legal characteristics of the "new legal order" created by the founding treaties of the EU, which are unlike ordinary international treaties: see paras. 157-158, where the Court referred to the legal order having a nature "which is peculiar to the EU". At para. 176, the Court referred to the judicial system conceived by the treaties, which has as its "keystone" the preliminary ruling procedure in Article 267 of the Treaty on the Functioning of the European Union.

156. Thirdly, we must bear in mind that the UK is no longer a member of the EU. The 2018 Act carefully sets out the scheme by which this Court continues to be bound by retained EU law, including case law, but that does not apply to a judgment of the ECtHR. It is common ground that, if the judgment in *Big Brother Watch* had been given by the CJEU, it would not be binding on this Court, because it was given in May 2021, after the end of the implementation period on 31 December 2020. This Court would still be entitled to take it into account but the legal status of a judgment of the CJEU after 31 December 2020 is that it is no longer binding on this Court.

157. In those circumstances, we are not prepared to accept that Mr Jaffey can achieve indirectly, by relying on a judgment of the ECtHR, that which he cannot achieve directly, by relying on a judgment of the CJEU.

158. Finally, we bear in mind that the Government has already stated that it intends to amend the IPA in order to address the defects which were identified by the Grand Chamber in *Big Brother Watch*: see the written Ministerial Statement of 31 March 2022. In those circumstances, it would not be appropriate for this Court to anticipate exactly how the Government and Parliament of the UK must act in order to comply with the judgment in *Big Brother Watch*.

Remedies

159. We have not yet received final submissions on the issue of remedies, since it was agreed that it would be better to leave this issue over until after the parties had had the opportunity to consider whether the substantive claim for judicial review had succeeded in any respect.

160. The Claimant has reminded this Court that, generally speaking, the ordinary course which the Court will take is to grant an appropriate declaration which declares what

the law is and always has been: see e.g. *Ahmed v HM Treasury* [2010] UKSC 5; [2010] 2 AC 534, at 689, paras. 1-8 in the second judgment of Lord Phillips PSC. It is common ground, however, that the Court has the power to suspend the effect of a declaration in respect of retained EU law.

161. In *Open Rights Group* the Court of Appeal held that, where a provision of domestic law is found to be inconsistent with a rule of retained EU law, the domestic courts have the power identified in the jurisprudence of the CJEU to delay or suspend the disapplication of the inconsistent domestic legislation. Such power is limited to permitting a temporary suspension and should be exercised only exceptionally, on the basis of overriding considerations of legal certainty. In order for a suspension to be justified, such considerations have to be so compelling that it is necessary for them to take priority over the need to implement the dominant rule of retained EU law and disapply the subordinate provision of domestic law; therefore both the decision to suspend and the duration of any suspension need clear justification. The suspension should last no longer than is strictly necessary in order to avoid legal uncertainty. That was in substance the approach which this Court had taken in the 2018 judgment, which was considered and approved by the Court of Appeal in *Open Rights Group*.

162. We invite the parties to make written submissions as to the appropriate remedy which this Court should grant in the following order. The Defendants shall file and serve their written submissions by 7 July 2022. The Claimant shall then file and serve written submissions by 14 July 2022. The Court intends to make its final decision thereafter in writing but, should it become necessary, it will hold a further hearing.

163. Having regard to the principles set out in *McDonald v Rose* [2019] EWCA Civ 4; [2019] 1 WLR 2828, in particular at paras. 21-22, we adjourn the "decision hearing" for the purposes of enabling the court to make its determination on remedies; and for the parties to make any consequential applications, including any applications for permission to appeal and to extend time for filing an appeal notice.

Conclusion

164. For the reasons we have given this claim for judicial review succeeds in one respect, in relation to Part 3 of the IPA, read with Part 4, but is otherwise dismissed. We adjourn the "decision hearing" with directions as set out at paras. 162-163 above.