

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

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 27/04/2018

Before :

LORD JUSTICE SINGH
and
MR JUSTICE HOLGATE

Between :

**The Queen on the application of The National
Council for Civil Liberties (Liberty)**

Claimant

- and -

(1) Secretary of State for the Home Department

Defendants

**(2) Secretary of State for Foreign and
Commonwealth Affairs**

Martin Chamberlain QC, Ben Jaffey QC and David Heaton (instructed by **Bhatt Murphy**)
for the **Claimant**

James Eadie QC, Gerry Facenna QC, Julian Milford and Michael Armitage (instructed by
the **Government Legal Department**) for the **Defendants**

Hearing dates: 27-28 February 2018

Judgment Approved

Lord Justice Singh :

Introduction

1. This is the judgment of the Court, to which both of its members have contributed.
2. This claim for judicial review concerns the compatibility of the Investigatory Powers Act 2016 (“the IPA” or “the 2016 Act”) with both European Union (“EU”) law and the European Convention on Human Rights (“ECHR”). For present purposes the Court has only been concerned with part of the claim and not the whole of it: the hearing before us concerned the challenge to the compatibility of Part 4 of the 2016 Act with EU law.
3. In particular this case concerns the power given to the Secretary of State by section 87(1) of the IPA to issue “retention notices” to telecommunications operators requiring the retention of data. It is important to note that this power relates to

retention and not *access* to such data. It is also important to note that, although the power affects a wide range of private information to do with communications, it does not concern the *content* of such communications, such as emails or text messages.

4. The IPA received Royal Assent on 29 November 2016. Part 4 was brought into force (although not in its entirety) on 30 December 2016 and substantially re-enacts the Data Retention and Investigatory Powers Act 2014 (“DRIPA”).
5. The present claim for judicial review was issued on 28 February 2017.
6. On 6 April 2017 the Defendants filed their summary grounds of resistance.
7. On 14 June 2017 Jeremy Baker J granted permission to challenge Part 4 of the IPA; stayed the rest of the claim; and required the Defendants to state by 5 July 2017 whether they conceded the challenge to Part 4.
8. On 7 July 2017 the Defendants conceded that Part 4 of the IPA is, in its current form, inconsistent with the requirements of EU law in two respects.
9. However, Part 4 has not yet been amended. It is proposed by the Government that amendments will be made by secondary legislation, under section 2(2) of the European Communities Act 1972, as amended, (“the ECA” or “the 1972 Act”), to be subject to the affirmative resolution procedure in Parliament. The Claimant contends that, in the meantime, unlawful retention of, and access to, communications data therefore continues.
10. The Claimant invites this Court to make an “order of disapplication” in respect of Part 4 insofar as it is conceded to be incompatible with EU law or is undefended. However, it further submits that the order of disapplication should be suspended until 31 July 2018. It submits that this would give the Government and Parliament a reasonable opportunity to introduce legislation which is compatible with EU law. The arguments in this regard evolved to some extent during the course of the hearing before us and we shall have to return to them later in this judgment.

Background

11. The origin of the problem in the present case can be traced back to Directive 2006/24/EC (the “Data Retention Directive”). That Directive was held by the Court of Justice of the European Union (“CJEU”) to be invalid as a matter of EU law in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Case C-293/12) EU:C:2014:238; [2015] QB 127.
12. In the United Kingdom the Data Retention Directive had been given effect by the Data Protection Regulations 2009. Because of the perceived invalidity of those Regulations Parliament acted swiftly to permit certain retention to continue to take place by enacting the DRIPA in 2014.
13. Section 1 of the DRIPA was the subject of challenge in the courts. That challenge succeeded before the Divisional Court (Bean LJ and Collins J): *R (Davies and Watson) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin); [2016] 1 CMLR 13 (“*Watson DC*”).
14. That decision was appealed by the Secretary of State. The Court of Appeal decided to make a reference to the CJEU: [2015] EWCA Civ 1185; [2016] 1 CMLR 48 (“*Watson CA 2015*”).

15. That reference was considered on an expedited basis by the CJEU and heard together with a reference which had been made by a Swedish Court in *Tele2 Sverige AB v Post-och telestyrelsen* (Case C-203/15).¹
16. The CJEU gave its judgment in those cases on 21 December 2016: EU:C:2016:970 (“*Watson* CJEU”).
17. The Court of Appeal then resumed its consideration of the *Watson* case and, after a hearing which took place on 8 December 2017, gave judgment on 30 January 2018: [2018] EWCA Civ 70 (“*Watson* CA 2018”). Although by that time the DRIPA had been repealed, the Court of Appeal granted a declaration that it was incompatible with EU law in two respects.
18. In the main judgment, which was given by Lord Lloyd-Jones, the Court confirmed that the two inconsistencies with EU law which are clear are that, in the area of criminal justice:
 - (1) access to retained data is not limited to the purpose of combating “serious crime”; and
 - (2) access to retained data is not subject to prior review by a court or an independent administrative body.
19. The Court of Appeal made a declaration that the DRIPA was incompatible with EU law in those two respects.

Material Provisions of the IPA

20. Section 61(7) of the IPA, which appears in Part 3, sets out the following purposes for obtaining communications data:
 - “(7) 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 purpose of preventing or detecting crime² or of preventing disorder,
 - (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 protecting public health,
 - (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,

¹ The *Watson* case had the reference number C-698/15.

² It will be seen this is not confined to “serious crime”.

- (g) 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,
- (h) to assist investigations into alleged miscarriages of justice,
- (i) 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 reason for P's death or condition, or
- (j) for the purpose of exercising functions relating to –
 - (i) the regulation of financial services and markets, or
 - (ii) financial stability.”

21. Part 4 of the IPA is headed “Retention of Communications Data”. Section 87(1) provides that:

“The Secretary of State may, by notice (a “retention notice”) and subject as follows, require a telecommunications operator to retain relevant communications data if –

- (a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7) (purposes for which communications data may be obtained), and
- (b) the decision to give the notice has been approved by a Judicial Commissioner.”³

22. In Part 4 “relevant communications data” has the following meaning, according to section 87(11):

³ Although the first part of section 87(1) has been brought into force, para. (b) is not yet in force.

“In this Part ‘relevant communications data’ means communications data which may be used to identify, or assist in identifying, any of the following –

- (a) the sender or recipient of a communication (whether or not a person),
- (b) the time or duration of a communication,
- (c) the type, method or pattern, or fact, of communication,
- (d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or
- (e) the location of any such system,

and this expression therefore includes, in particular, internet connection records.”

23. Although this covers a wide range of private information, it is important to note that it does not include the *content* of communications, for example emails or text messages.

Relevant Provisions in the EU Charter of Fundamental Rights

24. Article 6(1) of the Treaty on European Union provides that the EU Charter of Fundamental Rights shall have “the same legal value” as the Treaties.

25. Article 7 of the Charter provides that:

“Everyone has the right to respect for his or her private and family life, home and communications.”

26. Article 8 concerns protection of personal data and provides that:

- “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.”

27. Article 11 concerns freedom of expression and information. It provides that:

“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.

2. The freedom and pluralism of the media shall be respected.”

28. Article 51, which concerns the field of application of the Charter, provides that the provisions of the Charter are addressed both to the institutions of the EU “and to the Member States only when they are implementing Union law.” Article 51(1) continues:

“... They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.”

29. Article 52 of the Charter provides as follows:

“Scope and interpretation of rights and principles.

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 [European] 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.”

The development of the arguments as to the appropriate remedy

30. As we have mentioned, in the light of the decision of the CJEU in *Watson*, the Defendants have accepted that Part 4 of the 2016 Act is incompatible with EU law in two respects and must therefore be amended.

31. As we have also mentioned, in *Watson* CA 2018, the Court of Appeal made a declaration that the DRIPA was incompatible with EU law in two respects which are in essence the subject of the concession now made by the Defendants in respect of Part 4 of the IPA. However, it is important to bear in mind that, by the time that declaration was made, the DRIPA had already been repealed by Parliament and replaced with the IPA. Therefore the declaration made by the Court related to a past incompatibility; it did not have the effect of disapplying any legislation currently in force.
32. In the present proceedings, the Defendants submit that no more than declaratory relief is required in respect of Part 4 of the 2016 Act in similar terms to the declaration granted by the Court of Appeal in *Watson* CA 2018. In particular the Defendants resist any suggestion on behalf of the Claimant that the Court should disapply the current legislation, even with such an order of disapplication having only suspended effect. Finally, there is a dispute between the parties as to the period of suspension should the Court decide to make an order of disapplication at all.
33. However, as we have mentioned, the arguments evolved in an important way during the course of the hearing before this Court. When making his reply on behalf of the Claimant, Mr Chamberlain QC asked the Court to make a declaration in the following terms:

“Part 4 of the Investigatory Powers Act 2016, read in accordance with the European Communities Act 1972, does not authorise the issue to a telecommunications operator of a retention notice requiring it to retain relevant communications data.”
34. In our judgement, there are several difficulties with that request, quite apart from the fact that it was made late in the day and had not been formulated in that way previously.
35. First, the wording of the draft declaration is so broad that it would include areas which are outside (or potentially outside) the area of serious crime: for example, the area of national security. As will become apparent later, the issue of whether the area of national security falls within the scope of EU law at all is the subject of dispute between the parties. It is, moreover, the subject of the first question which has been referred by the Investigatory Powers Tribunal (“IPT”) for determination in a preliminary ruling by the CJEU: see its decision of 8 September 2017 in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others* (IPT/15/110/CH).
36. Secondly, the draft wording is tantamount in substance to requiring disapplication of Part 4 of the Act with *immediate* effect. In our view, that would be to grant the Claimant in this case a remedy which not only has never previously been sought but is one which the Claimant has expressly disavowed it was seeking in the past. For that purpose it is necessary to rehearse some of the procedural history of these proceedings.
37. When, on 14 June 2017, Jeremy Baker J granted permission for the claim in relation to Part 4 of the 2016 Act to proceed to a substantive hearing he made a direction (at

para. 2) that by 5 July 2017 the Defendants should set out in writing whether they intended to concede or contest the claim in relation to Part 4.

38. The relevant letter was in fact dated 7 July 2017. In that letter the Government Legal Department said on behalf of the Defendants that they “do not contest the claim that Part 4 of the IPA is, in its current form, inconsistent with the requirements of EU law insofar as:

(1) it does not ensure that, in the area of criminal investigations, access to and use of retained communications data is restricted to the objective of fighting serious crime; and

(2) access to retained data is not subject to prior review by a court or an independent administrative body. Accordingly, the Defendants would not contest the making of a declaration that Part 4 of the IPA in its present form is inconsistent with EU law on these grounds.”

It should be noted that there was an important footnote attached to that proposition:

“The Defendants’ position is without prejudice to the question of the application of EU law in a national security context, which is currently under consideration by the Investigatory Powers Tribunal.”

39. In the same letter it was said that the Defendants did not, however, consider that the Claimant was entitled to any further order. It was added that, for the avoidance of doubt:

“The Defendants would resist any application for an Order that required the disapplication of any aspect of the current legislation before Parliament has been given an opportunity to amend the legislation to comply with EU law as clarified by the CJEU.”

40. In the concluding section of the letter, it was said:

“As it is common ground in this claim (as in *Watson*) that no aspect of the current regime should be immediately disappplied, and that Parliament must be given an opportunity to amend the scope of the legislation to bring it into line with EU law, there is no basis at this stage for any relief beyond a declaration.”

Further it was said:

“For the avoidance of doubt, pending amendment of the legislation by Parliament the Secretary of State will continue to operate the current arrangements under Part 4 of the Act, including where that is necessary in order to ensure that communications data is retained following the expiry of the transitional arrangements for retention notices issued under s.1 DRIPA.”

41. The Claimant's solicitors replied to that letter on 13 July 2017. They noted that the Defendants accepted that Part 4 is incompatible with EU law but took the view that:

“This stance is contrary to law and shows a disregard for the rights to privacy of citizens.”

This was because the Defendants had made it clear that they would continue to operate the current arrangements for an undefined and potentially unlimited period. It was that issue of timing which was the subject of objection by the Claimant at that time.

42. It was suggested by the Claimant's solicitors that the Defendants' position required further clarification. At paras. 10-14 of the letter they set out what relief they contended the Claimant was entitled to and headed it “Order for Disapplication.” They enclosed a draft order which they said their client could agree. They noted that the terms of the declaration they considered should be made reflected the judgment of the CJEU in *Watson*. Further, and importantly, they suggested that the order sought was in line with that made by the Divisional Court in *Watson* and that:

“There is no plausible point of distinction.”

They contended that it is the Court's duty to give effect to EU law, including by disapplying incompatible provisions. They also noted that the Defendants had not argued before the Court of Appeal, when *Watson* returned from the CJEU, that the order for disapplication should not have been made by the Divisional Court. Further, the letter contended that the Defendants' concerns about the need for Part 4 powers in arresting and prosecuting criminals and preventing attacks “can be accommodated by an appropriate suspension of the order for disapplication, as again was the case in *Davis & Watson*.” In our view, that was a realistic and fair acknowledgement that, in this context, it cannot reasonably be expected that there should, immediately, be no legislation at all in place allowing retention of data that is needed to apprehend criminals or prevent terrorist attacks; what the Claimant was seeking was a reasonable period in which the legislation could be amended.

43. The letter continued that they agreed that the legislation must be amended but the absence of any defined period in which the ongoing unlawful conduct will come to an end is impossible to reconcile with the duty on a Member State's courts to give full effect to EU law. They recorded that:

“You observe that it is common ground that Part 4 should not be immediately disapplied.”

They did not in terms dissent from that suggestion on the part of the Defendants and appeared to agree with it because the letter continued:

“That is merely a reason for a *suspended* order for disapplication, as in *Davis & Watson*. It does not suggest that no order for disapplication should be made.” (Italics in original)

Finally the letter continued:

“The utility of a suspended order for disapplication lies in the practical requirement it imposes to enact changes to legislation within the specified time. Given the length of time that has passed since this claim was brought in February 2017 and the absence of any firm proposals for amendment, that is vital in this case.”

44. It is clear therefore that that was the form of the remedy which was being sought at that time by the Claimant. That is the claim which the Defendants had to meet. In their detailed grounds of resistance (dated 11 December 2017) they invited the Court to dismiss the Claimant’s challenge based on EU law save to the extent encompassed by the Defendants’ concession. Further, they said:

“As to the matters falling within the scope of the Defendants’ concession, no relief beyond declaratory relief is appropriate or necessary, given that those matters are already being addressed by proposed amendments that have been published for consultation and will in due course be considered by Parliament.” (para. 137)

45. We have rehearsed the procedural history in detail because this is more than simply a pleading point, although the importance of having a properly pleaded case and response to it should not be underestimated in judicial review proceedings.
46. But the point goes further than that. This is a very important constitutional case, in which there are vital public interests at stake on each side of the argument. For reasons that we set out more fully later, we have reached the clear view that, whatever other remedy should be granted in this case, the Court should not do anything which would have the effect of immediately disapplying Part 4 of the 2016 Act, with the resultant chaos and damage to the public interest which that would undoubtedly cause in this country.
47. Before we return to the question of what remedy, if any, should be granted in the present case to reflect what are acknowledged to be inconsistencies between Part 4 of the IPA and EU law, it is necessary to consider in some detail (i) the power of the Court to grant a declaration; and (ii) the way in which the doctrine of the supremacy of EU law has come to be received into the domestic law of this country, which has otherwise recognised the legislative supremacy of Parliament.

The power to grant a declaration

48. The history and development of the Court’s power to grant a declaration is discussed in Zamir and Woolf, The Declaratory Judgment (4th ed., 2011), Ch. 2. For present purposes it will suffice to note that the power to grant a declaration, even if no other remedy is sought, was conferred by the Rules of the Supreme Court 1883 in Order 25, Rule 5. That was replaced by the Rules of the Supreme Court 1965, Order 15, Rule 16, which stated:

“No action or other proceeding shall be open to objection on the ground that a merely declaratory judgment or order is sought thereby, and the court may make binding declarations of right whether or not any consequential relief is or could be claimed.”

49. The current power of the Court is governed by the Civil Procedure Rules 1998, as amended, and in particular Rule 40.20, which states:

“The Court may make binding declarations whether or not any other remedy is claimed.”

50. It is to be noted that the phrase now is “binding declarations” and there is no longer any reference to a declaration “of right”.

51. Nevertheless, what is significant is that a declaration is binding. This is unsurprising given its function in our legal system. As Zamir and Woolf put it, at para. 1-02:

“A declaratory judgment is a formal statement by a court pronouncing upon the existence or non-existence of a legal state of affairs. It is to be contrasted with an executory, in other words coercive, judgment which can be enforced by the courts. ... A declaratory judgment ... pronounces upon a legal relationship but does not contain any order which can be enforced ...”

52. There is a constitutional convention that the executive will comply with a declaration made by the court even though it does not have coercive effect. For example, in *R v Secretary of State for Transport, ex p. Factortame Ltd* [1990] 2 AC 85, at p.150, Lord Bridge of Harwich said:

“The form of final relief available against the Crown has never presented any problem. A declaration of right made in proceedings against the Crown is invariably respected and no injunction is required.”

53. However, it is important to note what is said by Zamir and Woolf, at para. 1-07:

“... Whilst the defendant is assumed to have respect for the law, justice does not rely on this alone. A declaration by the court is not a mere opinion devoid of legal effect: the controversy between the parties is determined and is *res judicata* as a result of the declaration being granted.”⁴

⁴ As is noted by Zamir and Woolf, at fn.9 on p.4, the doctrine of *res judicata* does not strictly apply in public law cases. However, the court could act to prevent an abuse of power by the executive.

54. When Order 53 of the Rules of the Supreme Court was reformed in 1977 to create the new procedure of “an application for judicial review” it provided for the grant of a declaration in such an application. Order 53, Rule 1(2) provided:

“An application for a declaration or an injunction ... may be made by way of an application for judicial review, and on such an application the court may grant the declaration or injunction claimed if it considers that, having regard to –

(a) the nature of the matters in respect of which relief may be granted by way of an order of mandamus, prohibition or certiorari,⁵

(b) the nature of the persons and bodies against whom relief may be granted by way of such an order, and

(c) all the circumstances of the case, it would be just and convenient for the declaration or injunction to be granted on an application for judicial review.”

55. In 1981 Parliament enacted primary legislation to govern applications for judicial review: at that time the statute was called the Supreme Court Act 1981 but has since been renamed the Senior Courts Act 1981. Section 31(2) of that Act sets out the circumstances in which the Court may grant a declaration in an application for judicial review.

56. The procedure for bringing claims for judicial review, as they are now known, is governed by Part 54 of the Civil Procedure Rules. Rule 54.3(1) provides that the judicial review procedure “may be used” in a claim for judicial review where the claimant is seeking a declaration. Where the claimant is seeking a declaration in addition to one of the remedies listed in Rule 54.2 (for example a quashing order) the judicial review procedure “must be used”.

57. We now turn to how the general power to grant a declaration has come to be used in the context of a challenge to primary legislation under EU (formerly Community) law. In particular it is necessary to see how the doctrine of the supremacy of EU law has been received into domestic law.

The reception of the doctrine of the supremacy of EU law into domestic law

58. The doctrines of direct effect of certain norms of EU law and the supremacy of EU law were well-established in the jurisprudence of the European Court of Justice before 1973, when the UK became a member of what was then called the European Economic Community. The way in which these concepts were given effect in domestic law was by section 2 of the European Communities Act 1972 (“ECA” or “the 1972 Act”). So far as material, section 2 provides:

“(1) All such rights, powers liabilities, obligations and restrictions from time to time created or arising by or under the Treaties, and all

⁵ These old names for the prerogative orders have now been replaced by more modern terminology: for example, certiorari is now a “quashing order”.

such remedies and procedures from time to time provided for by or under the Treaties, as in accordance with the Treaties are *without further enactment to be given legal effect* or used in the United Kingdom *shall be recognised and available in law*, and be enforced, allowed and followed accordingly; and the expression ‘enforceable EU right’ and similar expressions shall be read as referring to one to which this subsection applies.

...

(4) The provision that may be made under subsection (2) above includes, subject to Schedule 2 to this Act, any such provision (of any such extent) as might be made by Act of Parliament, and *any enactment passed or to be passed*, other than one contained in this part of the Act, *shall be construed and have effect subject to the foregoing provisions of this section*; but, except as may be provided by any Act passed after this Act, Schedule 2 shall have effect in connection with the powers conferred by this and the following sections of this Act to make Orders in Council or orders, rules, regulations or schemes.” (Emphasis added)

59. In *R v Secretary of State for Employment, ex p. Equal Opportunities Commission* [1995] 1 AC 1 (“*EOC*”), at pp.26-27, the House of Lords had to consider an argument made on behalf of the Secretary of State that RSC Order 53, Rule 1(2), which gave the Court power to make declarations in judicial review proceedings, was only applicable where one of the prerogative orders would be available under Rule 1(1). In particular it was submitted that, since the prerogative orders could not be made in respect of an Act of Parliament (for example, an Act of Parliament could not be quashed by a court by an order of certiorari), nor could a declaration be made.
60. The House of Lords rejected that argument. Lord Keith of Kinkel said, after consideration of the *Factortame* series of cases, where the applicants had sought a declaration that the provisions of Part II of the Merchant Shipping Act 1988 should not apply to them on the ground that this would be contrary to European Community law:
- “The effect was that certain provisions of United Kingdom primary legislation were held to be invalid in their purported application to nationals of Member States of the European Economic Community, but without any prerogative order being available to strike down the legislation in question, which of course remained valid as regards nationals of non-Member States. At no stage in the course of the litigation, which included two visits to this House, was it suggested that judicial review was not available for the purpose of obtaining an adjudication upon the validity of the legislation insofar as it affected the applicants.”
61. Lord Keith continued:

“The *Factortame* case is thus a precedent in favour of the EOC’s recourse to judicial review for the purpose of challenging as incompatible with European Community law the relevant provisions of the Act of 1978 [the Employment Protection (Consolidation) Act 1978].

...

A declaration that the threshold provisions of the Act of 1978 are incompatible with Community law would suffice for the purposes sought to be achieved by the EOC and is capable of being granted consistently with the precedent afforded by *Factortame*. ... The EOC is concerned simply to obtain a ruling which reflects the primacy of European Community law enshrined in section 2 of the Act of 1972 and determines whether the relevant United Kingdom law is compatible with the Equal Pay Directive and the Equal Treatment Directive.”

62. Although the House of Lords used the phrase “declaration of incompatibility” in the *EOC* case, it was using that phrase before the Human Rights Act 1998 (“HRA”) was enacted. More importantly, it was using that phrase in a sense which is different from the concept of a declaration of incompatibility which may be granted under section 4 of the HRA. Under the scheme of the HRA a declaration of incompatibility with Convention Rights does not affect the validity, continuing operation or enforcement of the provision of primary legislation in respect of which it is given: see section 4(6) (a). Moreover, such a declaration is not binding even on the parties to the proceedings in which it is made. It is therefore a unique and novel kind of remedy which Parliament has created. Parliament has also made it clear that it can only be made by courts of a certain seniority in the legal system: in England and Wales the High Court and above. Without in any way wishing to underestimate the practical or political significance of a declaration of incompatibility under section 4 of the HRA, we would note that the only legal effect of such a declaration is to provide a Minister with the power to make a “remedial order” under section 10 of the HRA. This means in effect that primary legislation can be amended by a Ministerial order.
63. In our view, a declaration of incompatibility under the HRA is significantly different from a binding declaration as envisaged by the general law and, in particular, in the context of EU law by the House of Lords in the *EOC* case.
64. As Lord Keith made clear in the *EOC* case, courts in this country have no power to “strike down” an Act of Parliament. However, it is also clear that there may be a duty on courts in this country to “disapply” incompatible domestic legislation, even primary legislation, to the extent of that inconsistency with directly effective EU law. As has subsequently been explained in the House of Lords, the relevant legislative provision “is not made void but it must be treated as being ... ‘without prejudice to the directly enforceable Community rights ...’ ”: see *Fleming (trading as Bodycraft) v HMRC* [2008] UKHL 2; [2008] 1 WLR 195, at para. 24 (Lord Walker of Gestingthorpe). As Lord Walker put it, at para. 62:

“... The disapplication of offending legislation is the duty of the national court, even if it involves action which would

otherwise be alien to the strong judicial instinct not to intrude on the province of the legislature.”

As Lord Walker went on to make clear in the same passage, jurisprudence under section 3 of the HRA is in this context “irrelevant and misleading”. Rather the guiding principles are those set out in the “seminal judgment” of the ECJ in *Amministrazione delle Finanze dello Stato v Simmenthal SpA* (Case C-106/77) [1978] ECR 629.

65. In one sense, this is a rule of interpretation. The incompatible legislation may still continue to have effect, for example, where it can properly be applied (compatibly with EU law) in respect of persons who are not entitled to the benefit of directly enforceable EU rights. An example of that can be found in the decision of the House of Lords in *Imperial Chemical Industries Plc v Colmer (Inspector of Taxes) (No. 2)* [1999] 1 WLR 2035, at p.2041.

66. However, as Lord Walker explained, referring to the *ICI* case, in *Autologic plc v IRC* [2005] UKHL 54; [2006] 1 AC 118, at para. 128:

“... It is not a matter of construing the taxing statute, but of determining whether it is overridden by a rule from a higher legal order which gives the taxpayer companies a restitutionary claim.”

67. This is why, as Lord Walker explained in *Fleming*, at para. 25:

“... Only in the most formal sense (because of the terms of section 2(4) of the European Communities Act 1972) can disapplication be described as a process of construction.”

68. As Lord Walker said, the exercise of “[d]isapplication of national legislation is an essentially different process from its interpretation so as to conform with EU law.” Further, as Lord Walker explained in the same passage:

“Disapplication is called for only if there is an inconsistency between national law and EU law.”

69. The position was summarised succinctly by the Supreme Court in the majority judgment in *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5; [2018] AC 61, at para. 67:

“... Following the coming into force of the 1972 Act, the normal rule is that any domestic legislation must be consistent with EU law. In such cases, EU law has primacy as a matter of domestic law, and legislation which is inconsistent with EU law from time to time is to that extent ineffective in law.”

70. In the same passage the majority judgment described the 1972 Act as having “a constitutional character”. Those statements of principle are now well established in the law of this country and reflect a long line of authority in the House of Lords and the Supreme Court.
71. In *R (Buckinghamshire County Council) v Secretary of State for Transport* [2014] UKSC 3; [2014] 1 WLR 324, at para. 206, Lord Neuberger PSC and Lord Mance JSC said:
- “Under the European Communities Act 1972, United Kingdom courts have also acknowledged that European law requires them to treat domestic statutes, whether passed before or after the 1972 Act, as invalid if and to the extent that they cannot be interpreted consistently with European law ... That was a significant development, recognising the special status of the 1972 Act and of European law and the importance attaching to the United Kingdom and its courts fulfilling the commitment to give loyal effect to European law. ...”
72. At para. 207, they noted that, although the United Kingdom has no written constitution, it does have a number of “constitutional instruments” and that amongst those can be included the European Communities Act 1972.
73. It is implicit in what we have said so far that the constitutional status of the 1972 Act has the consequence that the doctrine of “implied repeal”, which would otherwise apply under our constitutional law, has been abrogated by the European Communities Act. In other words, even an Act of Parliament passed after the 1972 Act is made subject to its legal effect, as indeed was the case in the *EOC* case itself. Express repeal by Parliament of the European Communities Act is available to it. As is well-known, the people of the United Kingdom voted in a referendum held on 23 June 2016 to leave the EU and in March 2017, with the assent of Parliament, the Government gave notice under Article 50 TEU that this country will leave the EU. However, unless and until Parliament repeals the 1972 Act, the consequences of it, including the primacy of EU law, continue to apply in this country.
74. Nevertheless, it seems to us that a fundamental question which has to be addressed in cases such as the present is: what exactly is the nature and extent of the incompatibility of national legislation with directly effective EU law? Sometimes, the incompatibility may consist of a provision in national legislation which can simply be ignored or regarded as overridden by the relevant norm of EU law. For example, if national legislation imposes a procedural threshold before a person can bring a claim in the Employment Tribunal of working for at least 16 hours per week (the sort of condition which there was in the *EOC* case), the consequence of incompatibility with directly effective rights in EU law (such as the right not to be discriminated against) may simply be that the procedural threshold in national law is to be ignored and will not operate as a matter of law to prevent the claim being properly lodged in the Employment Tribunal. That action by a court or tribunal does not on analysis require any order to be made by it. Often the court will make an appropriate declaration but it may be that the relevant court or tribunal has no jurisdiction to make even a declaration. It will still be under a duty to disapply the incompatible national legislation. The court or tribunal simply regards the rule of national law as being ineffective to the extent of its incompatibility with directly effective EU law.

75. In the present case, however, in our view, the nature and extent of the incompatibility with EU law which the Defendants accept does not go that far. As a matter of principle, there is nothing in EU law which prevents a Member State from having in place national legislation which permits the retention of data (to meet the crime objective) along the lines of the 2016 Act. The incompatibility which has been identified by the CJEU and is accepted by the Defendants consists of two failures to have certain safeguards in the legislation concerned. Correcting those failures will require positive steps to be taken by way of amending legislation. On any view, that was always bound to take some time. We are unable to reach the view that, from the moment when the incompatibility was pronounced by the CJEU or when it was acknowledged by the Defendants in this country, the national legislation had as a matter of absolute obligation to be disapplied immediately. That would, as Mr Eadie QC submitted on behalf of the Defendants, be a recipe for chaos.
76. These are deep constitutional waters, in which the courts of this country have been and still are feeling their way. In our judgement, the appropriate and principled approach is for the Court to allow both the Government and Parliament a reasonable amount of time in which they have the opportunity to enact national legislation to correct the defects which exist and which are incompatible with EU law. That was, as we understand it, implicit in the Claimant's own approach to this important and difficult issue as the case was originally put. We consider that was a sensible approach as a matter of principle.
77. In our view, courts in this country should proceed with great caution in a context such as this. This is for two reasons. First, the practical implications would, as we have indicated, be enormous and potentially damaging to the public interest. Secondly, this is relatively uncharted territory for courts in this country, possibly in contrast to courts in other countries which have a much longer history of constitutional adjudication in which even primary legislation can be challenged.
78. The need for a cautious approach is supported by the dicta of Lord Mance JSC in *R (Chester) v Secretary of State for Justice* [2013] UKSC 63; [2014] AC 271, at paras. 72-74. That case arose from the prohibition on voting by any convicted person while serving their sentence: see section 3(1) of the Representation of the People Act 1983 and section 8 of the European Parliamentary Elections Act 2002. In relevant part that case was brought by prisoners who had been convicted of murder and were serving life sentences on the basis of Article 3 of the First Protocol to the European Convention on Human Rights, which is one of the Convention rights set out in Sch. 1 to the HRA. However, as we have mentioned earlier, the only remedy which can be granted by a court under the HRA, if it is found that primary legislation is incompatible with a Convention right, is a declaration of incompatibility. Section 4 of the HRA makes it clear that such a declaration is not binding. Nor does the Court have any power to disapply primary legislation if it is incompatible with a Convention right.
79. Against that background the prisoners in that case also sought to rely on their rights in EU law, in particular Article 20(2)(b) of the Treaty on the Functioning of the European Union ("TFEU"), and Article 40 of the Charter of Fundamental Rights of the EU. It was held by the Supreme Court that those provisions did not apply to Scottish parliamentary elections, since they were not "municipal" elections; and that, in relation to EU and municipal elections, EU law does not confer an individual right to vote which parallels that recognised by the jurisprudence of the European Court of Human Rights under the Convention. The Court held that, under the Treaties governing the EU, eligibility to vote is a matter for national parliaments; provisions

concerning individual voting rights relate only to concerns of equality as between nationals of a Member State and free movement within the EU; and so only apply to citizens resident in a state other than their own state of nationality.

80. In those circumstances, it was strictly unnecessary for the Supreme Court to say anything about remedies, since it held that there was no breach of any rights in EU law in the event. However, it is important to note that Lord Mance did go on to express the *obiter* view that, even if EU law did recognise an individual right to vote:

“... the only relief that could be considered under domestic law would be a generally phrased declaration that the legislative provisions governing eligibility to vote in European Parliamentary and municipal elections in the United Kingdom were inconsistent with European Union law. Thereafter, it would be for the United Kingdom Parliament to address the position and make such legislative changes as were considered appropriate. ...” (Para. 72)

81. Lord Mance continued, at para. 73:

“I reject the submission that the Supreme Court could or should simply disapply the whole of the legislative prohibition on prisoner voting, in relation to European Parliamentary and municipal elections, thereby making all convicted prisoners eligible to vote pending fresh legislation found to conform with European Union law. It is clear from both *Hirst (No.2)* and *Scoppola* that, under the principles established by those cases, a ban on eligibility will be justified in respect of a very significant number of convicted prisoners.”

82. Finally in this context, at para. 74, Lord Mance said:

“... It would also be impossible for the Supreme Court itself to devise an alternative scheme of voting eligibility that would or might pass muster in a domestic or supra-national European court. Equally, the court could not determine or implement the practical and administrative arrangements that would need to be made to enable any convicted prisoners eligible under any such scheme to have the vote. Such matters would be beyond its jurisdiction. In the domestic constitutional scheme, any scheme conferring partial eligibility to vote on some convicted prisoners is quintessentially a matter for the United Kingdom Parliament to consider, determine and arrange. ... [T]he Court of Justice made clear that it is only ‘within the limits of its jurisdiction’ that a national court can be expected to provide the legal protection that European Union law requires. That being so, the creation of a new scheme must be a matter for the United Kingdom Parliament.”

83. Mr Chamberlain is entitled to submit that those *obiter dicta* were uttered in a context where it was clear, on the jurisprudence of the European Court of Human Rights, that it would be open to Parliament to continue to prohibit prisoners of the kind involved in that case (those guilty of very serious offences) from voting. However, what that case demonstrates is that (1) there is no automatic rule that, once it is held or conceded that a provision of primary legislation is incompatible with EU law, the national legislation must immediately be disapplied; and (2) what is crucial is the nature of the incompatibility.
84. It may be that, in appropriate contexts, a provision in primary legislation is so clearly, inherently and absolutely incompatible with EU law that it must be disapplied to the extent of its inconsistency with EU law. Examples of such legislation may include the absolute ceiling on compensation in sex discrimination cases which existed at one time in national law and was held to be incompatible with European Community law in *Marshall v Southampton and South West Hampshire AHA* [1986] ICR 335; and the minimum threshold of 16 hours or more per week to be worked by an employee before she could bring a claim for unfair dismissal, which was the subject of the decision of the House of Lords in the *EOC* case. As those cases make clear, there can be circumstances in which a domestic court or tribunal has a duty to disapply a provision in national law (even if contained in primary legislation) when it is incompatible with EU law. However, in such situations, the court or tribunal is quite simply disapplying the inconsistent rule of national law. It is not required to set up some alternative scheme.
85. In the present context, it seems to us, there clearly will be a need for an alternative scheme which corrects the two defects in the current legislation which the Defendants accept in the light of the judgment of the CJEU in *Watson*. In our view, there are strong constitutional reasons, and not only practical ones, for declining to grant any order or declaration which would have the effect of immediately disapplying the provisions of Part 4 of the 2016 Act.
86. Against that background of principle we return to the issue of what remedy should be granted in the present case. Two questions remain to be addressed under that heading:
- (1) Should the remedy to be granted be a declaration or what was called by the Divisional Court in *Watson* DC an “order for disapplication”?
 - (2) Whichever of those remedies should be granted, should the Court grant that remedy with immediate effect or should it suspend the order?
87. A subsidiary question which arises under question (2) is the period of time for which any remedy granted by the Court should be suspended. The Claimant submits that it should be no later than 31 July 2018. The Defendants submit that it should be no earlier than 1 April 2019.

The Appropriate Remedy

88. In *Watson* DC the Divisional Court made an order of disapplication in respect of section 1 of the DRIPA. Whether that was an order that was correctly made does not seem to have been the subject of argument in the Court of Appeal but, in any event, that Court did not need to consider whether to make such an order because, by the time of its decision in January 2018, the DRIPA had been repealed. As we have

mentioned earlier, the Court granted a declaration that the DRIPA was incompatible with EU law in two respects but this had no effect on any current legislation.

89. It is important to recall that the Divisional Court is not a single court, like the Court of Appeal. It is simply a panel of the High Court which consists of more than one judge. Although a decision of an earlier Divisional Court will normally be followed by another Divisional Court, it is not strictly binding on it: *R v Manchester Coroner, ex p. Tal* [1985] QB 67, at pp.79-81 (Robert Goff LJ).
90. We have had the benefit of more detailed submissions on the appropriate remedy which should be granted than the Divisional Court appears to have done in 2015. We have also had the advantage of seeing how the Court of Appeal approached the issue of remedy in *Watson* CA 2018. We have come to the conclusion that the appropriate remedy in the present case is not an order of disapplication but a declaration.
91. As we have mentioned, this case is on analysis closer to cases where there has been a breach of a positive obligation imposed on a Member State by EU law. There is therefore some similarity to the sort of situation with which the courts have had to grapple in the context of environmental protection. Our attention was drawn at the hearing to the decision of the Supreme Court in *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* [2015] UKSC 28; [2015] 3 CMLR 15. The analogy is not exact because that case concerned express requirements to produce an air quality plan in the shortest time possible: see Article 23(1) of Directive 2008/50/EC. Nevertheless, we consider that some assistance can be derived from that line of authority because, as subsequent decisions of this Court have made clear in implementing the decision of the Supreme Court, the Court has a role to play in ensuring that EU law is complied with within a reasonable time. As Lord Carnwath JSC said in the Supreme Court, EU law imposes an obligation on national courts to secure compliance with directly effective EU law and such matters cannot be left only to the European Commission: see para. 28. We also note that, at para. 30, Lord Carnwath said that the Court has “its own responsibility in the public interest” to provide an appropriate remedy in the circumstances.
92. As we have already said, we are not prepared to contemplate the grant of any remedy which would have the effect, whether expressly or implicitly, of causing chaos and which would damage the public interest.
93. Nor do we consider that any coercive remedy is either necessary or appropriate. This is particularly so in a delicate constitutional context, where what is under challenge is primary legislation and where the Government proposes to introduce amending legislation which, although it will be in the form of secondary legislation rather than primary, will be placed before Parliament for the affirmative resolution procedure to be adopted.
94. On the other hand it would not be just or appropriate for the Court simply to give the Executive a *carte blanche* to take as long as it likes in order to secure compliance with EU law. The continuing incompatibility with EU law is something which needs to be remedied within a reasonable time. As long ago as July 2017 the Defendants conceded that the existing Act is incompatible with EU law in two respects.
95. The Defendants submit that any time limit which the Court imposes should not be before April 2019. This is supported by the second and third witness statements of Mr Scurry and the letter of Sir Adrian Fulford (the Investigatory Powers

Commissioner or “IPC”) dated 27 February 2018, to which we have made reference in this Court’s judgment on procedural matters, in particular at para. 22.

96. We understand the practical difficulties to which that evidence refers. In particular we understand the reasons why both the IPC and the Defendants do not wish to establish the Office for Communications Data Authorisations (“OCDA”) in a way which proves to be premature and therefore counter-productive in the public interest.
97. However, we see force in the submissions made on behalf of the Claimant (in particular in their note of 2 March 2018, at para. 5). First, we see no reason why the *legal* framework cannot be amended before April 2019. In particular, it seems to us that *legal* limitations could be put on the retention of communications data by way of amending legislation much earlier than April 2019, even if the *practical* arrangements for the establishment of the OCDA need to wait until then. On any view, the legislation would have to be in place well before that date in order to be implemented.
98. Secondly, as the Claimant submits, the Judicial Commissioners appointed under the 2016 Act are already in post. On 18 October 2017 the IPC announced the appointment of 13 Judicial Commissioners, who are all either current or former members of the senior judiciary.
99. On the evidence which is before the Court at present, as we understand it, it has always been envisaged that amending legislation could be brought into force in July 2018. That would address the present incompatibility between Part 4 of the 2016 Act and EU law. Other aspects of the Act, such as Part 3, which deals with authorisation of access to data rather than its retention, may raise different considerations. Even if July 2018 is now too soon, we consider that a deadline of 1 November 2018 to have amending legislation in place would give the Defendants a reasonable amount of time to secure compliance with EU law. That will give the Government just over 6 months from the date of this judgment.
100. In all the circumstances of this case, therefore, we have come to the conclusion that the appropriate remedy to make in respect of what are acknowledged by the Defendants to be inconsistencies with EU law is to grant a declaration (i) specifying the two respects in which there is an incompatibility; and (ii) stating that those must be remedied within a reasonable time. Further, we propose to state in the declaration (iii) that a reasonable time would be 1 November 2018. We also propose to give the parties liberty to apply to vary the order or the terms of the declaration we grant if subsequent events (which must be supported by evidence) require any change to the timetable. If necessary this Court will hold a further hearing to consider any application if it is made.
101. We will now turn, more briefly, to each of the specific issues which were raised at the hearing before us.

(1) Other allegedly unlawful purposes

102. The Claimant submits that the order of disapplication which it seeks should also apply to those statutory purposes which are specified in section 61(7)(e), (f) and (j): those purposes are concerned with protecting public health, tax matters, and regulation of financial services/markets and financial stability. The Claimant submits that those purposes fall outside the scope of Article 15 of the e-Privacy Directive. The Claimant

also submits that the Defendants have failed to offer any substantive defence as to why these provisions in the IPA are compatible with EU law.

103. On behalf of the Defendants Mr Eadie submits that this is not an issue which the Court needs to resolve because the Government proposes to remove these purposes from the legislation in any event.
104. It is not entirely clear to us that the point was raised in terms in the Claimant's pleaded grounds of challenge: see paras. 171-178 of the statement of facts and grounds. Nevertheless, the point was raised in the Claimant's skeleton argument for the substantive hearing, at para. 24(3) and the Defendants responded at para. 10(c) of their skeleton argument.
105. In the circumstances which have arisen, where we have come to the view that the legislation will need to be amended within a reasonable time and in which the Defendants intend to exclude the relevant purposes from such amending legislation, we have come to the conclusion that the Court should not exercise its discretion to grant any remedy in respect of these matters, since none is necessary at this stage. Even if we had accepted the Claimant's submission that there should be an order of disapplication made, the Claimant accepts that such an order should be suspended. Accordingly, there is no need for an order of disapplication, nor even a declaration at this time.

(2) Application of *Watson* CJEU to the national security context

106. As we have already mentioned, the power conferred on the Secretary of State to issue a retention notice by section 87(1) of the IPA depends upon whether the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paras. (a) to (j) of section 61(7). Those purposes, which are listed in section 61(7) of the IPA, include (a) "in the interests of national security" and (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".
107. On behalf of the Claimant it is submitted that the safeguards which are required in accordance with the judgment in *Watson* CJEU apply not only to serious crime but also to retention/access of data for national security purposes.
108. On behalf of the Defendants it is submitted that national security falls outside the scope of EU law altogether and that the *Watson* CJEU requirements do not apply in that context. The Defendants place particular reliance on the terms of Article 4(2) TEU, which states that:

"... In particular, national security remains the sole responsibility of each Member State ..."
109. The Defendants also place reliance on the terms of Article 1(3) of the e-Privacy Directive, which is in the same terms as Article 3(2) of the Data Protection Directive, which provided:

"This Directive shall not apply to the processing of personal data ... in the course of an activity which falls outside the scope

of Community law, such as those provided for by titles V and VI of the [TEU] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) ...”

110. Although there is that dispute between the parties, the Claimant does not invite this Court to determine the question whether *Watson* CJEU applies in the national security context. Rather the Claimant invites this Court to make a reference to the CJEU under Article 267 TFEU for a preliminary ruling on that question.
111. In its judgment in *Privacy International* on 8 September 2017 the IPT referred two questions for a preliminary ruling by the CJEU:
- “1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the ‘e-Privacy Directive’), does a requirement in a direction by the Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies (‘SIAs’) of a Member State fall within the scope of Union law and of the e-Privacy Directive?
2. If the answer to Question (1) is ‘yes’, do any of the *Watson* Requirements, 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 SIAs 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?”
112. In the light of the pending reference in the IPT proceedings, the Defendants submit that it is both duplicative and unnecessary for this Court now to make a reference on the application of EU law and, in particular, of the criteria in *Watson* CJEU, to the national security context.
113. On behalf of the Claimant Mr Chamberlain submits that, nevertheless, this Court should exercise its discretion to make a reference on this issue. He submits that the legislation which is the subject of the IPT proceedings (section 94 of the Telecommunications Act 1984 (“the 1984 Act”), which concerns the power to issue a direction to a telecommunications operator) is not in the same terms as Part 4 of the IPA. Mr Chamberlain also submits that it is possible, given the way in which the questions referred by the IPT are framed, that Question (2) may never be reached by the CJEU, since it only arises if the answer to Question (1) is “yes”.
114. It is common ground that this Court is not under a duty to make a reference to the CJEU but has a discretion to do so. In our view, this Court should not exercise its discretion to make a reference to the CJEU under Article 267 TFEU, for the following reasons.

115. First, the Court of Appeal in its decision in *Watson* CA 2018 clearly considered that:

“... The reference made by the IPT raises *squarely* the question whether the judgment of the CJEU in the present case and, in particular, the mandatory requirements identified in that judgment ... apply where the purpose is that of national security. ...”: see para. 10 in the judgment of Lord Lloyd-Jones (emphasis added).

As Lord Lloyd-Jones went on to say, at para. 12, after summarising submissions on behalf of the parties which are similar to the ones made in the present proceedings, the Court took the view that the disputed issue should not be resolved in that case in part in view of the controversy over this issue before the IPT and the fact that it is now the subject of a further reference to the CJEU by the IPT.

116. Secondly, in our view, although the terms of section 94 of the 1984 Act and the terms of Part 4 of the 2016 Act are not identical, the questions which have been referred by the IPT are not confined to the precise scope of section 94. Rather they raise broader questions about the scope of EU law, having regard to Article 4 TEU and Article 1(3) of the e-Privacy Directive; and also raise the particular question of whether any of the *Watson* CJEU requirements apply in the field of national security.

117. For those reasons we refuse the application by the Claimant to make a reference to the CJEU on this question. This part of this claim will be stayed pending the CJEU’s decision in the reference in the *Privacy International* case.

(3) General and Indiscriminate Retention of Data

118. This issue arises from paragraph 1 of the CJEU’s dispositif in *Watson*, where the Court decided that Article 15(1) of the e-Privacy Directive precludes national legislation for the purposes of fighting crime which provides for the “general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.”

119. In *Watson* CA 2018 the Court of Appeal refused to make a declaration applying the CJEU’s conclusion to DRIPA, paras. 22-26. A major factor in the Court’s decision was the fact that the reasoning of the CJEU which led to paragraph 1 of its dispositif was based upon the language of the Swedish legislation the subject of the reference in the *Tele2* case, and not the language of DRIPA (see paras. 4 and 26 (2)). Mr Jaffey accepted that this argument was not raised in relation to DRIPA. The Court of Appeal also pointed out that this part of the CJEU’s judgment remained a live issue in the present proceedings challenging Part 4 of the 2016 Act and should be dealt with in these proceedings.

120. In its skeleton, the Claimant asks the Court to order a reference to the CJEU of the issue whether Part 4 of the 2016 Act is incompatible with EU law because the scheme provides for the general and indiscriminate retention of data. The Defendants submit that when the legislation is read properly and as a whole, this issue should be resolved in their favour and is *acte clair*.

121. The Claimant places heavy reliance upon paras. 106, and 108-111 of the CJEU’s decision. To put these passages into context, it is plain that the CJEU was dealing with legislation which in the reference from Sweden required the general retention of

all manner of electronic communication and traffic data, for all subscribers and registered users, and without differentiation or limitation, for the purposes of investigating, detecting and prosecuting crime (para. 105 of *Watson* CJEU).

122. The CJEU has decided that Article 15(1) of the e-Privacy Directive allows a Member State to adopt as a preventative measure the targeted retention of traffic and location data, for fighting serious crime, provided that that retention is limited as to categories of data, the means of communication, the persons concerned, the period of retention, and to what is strictly necessary (para. 108). In order to satisfy that requirement, national legislation must lay down clear and precise rules governing the scope and application of a data retention measure *and* impose “minimum safeguards” to provide effective protection against the risk of misuse of personal data (para. 109). The retention of data must meet objective criteria that establish a connection between that data and the objective to be pursued, although the *conditions* which need to be satisfied may vary according to the *nature of the measures* taken to prevent, investigate, detect or prosecute serious crime (para. 110). Objective evidence should make it possible to identify “a public” whose data is likely to reveal at least an indirect link with serious criminal offences, to contribute to fighting serious crime or to prevent a serious risk to public security (para. 111).
123. The judgment went on to advise that limits *might* be set by using a “geographical criterion” where the national authority considers that there is, in one or more geographical areas, a high risk of preparation for or commission of serious offences. We agree with the Defendants’ submission (para. 59b of their skeleton) that this part of para. 111 of the CJEU’s judgment was not in any way prescriptive. It merely gave an example which, according to the facts of a particular situation, could be used to set the parameters of a measure for retention of data. The CJEU did not lay down any legal requirement that this approach must be used.
124. In summary, the effect of paras. 108-111 of the CJEU’s judgment is that member states may adopt legislation which *permits* decisions to be taken for the targeted retention of data which is (a) sufficiently connected with the objective being pursued, (b) is strictly necessary and (c) proportionate. We do not read the CJEU’s decision as requiring more detailed factors which may be relevant to the *application* of those tests to be enshrined in domestic legislation. The range of considerations affecting the need to require the retention of data may vary considerably when dealing with matters affecting national security, public safety and serious crime. It would be impractical and unnecessary to set out in detail in legislation the range of factors which may fall to be applied according to the circumstances of different cases.
125. We also note from para. 109 of the CJEU’s judgment that the satisfaction of the key requirements set out in para. 108 depends not only upon legislative rules governing the scope and application of retention measures, but also the imposition of “minimum safeguards.” It is the combination of these two aspects which should achieve effective protection against the risk of misuse of personal data.
126. Before considering Part 4 of the 2016 Act, it is necessary to have in mind the nature of the Swedish legislation which was the subject of paragraph 1 of the CJEU’s dispositif. Mr Jaffey accepted that that legislation had effectively “copied” the approach adopted in the Data Retention Directive. The legislation itself required all providers of electronic communication services to retain all data, the retention of which was required by that Directive. Accordingly, the Swedish legislation was liable to be found incompatible with EU law on the same basis as the Directive had already been found to be invalid in *Digital Rights Ireland* (see *Watson* CJEU at paras. 62-63,

97-101 and 103). It is of particular note that, as Mr Jaffey accepted, the requirements of the Swedish legislation were not qualified by either a necessity test or a proportionality test. The blanket nature of the requirement in the Swedish legislation imposed on all operators to retain data, precluded the possibility of any consideration being given to the nature of any connection between the data to be retained and the pursuit of the objective of fighting serious crime.

127. The scheme laid down in Part 4 of the 2016 Act is very different from the Swedish legislation. First, the Act does not contain a blanket requirement requiring the general retention of communications data. The Act does not itself impose any requirement on telecommunications operators to retain data. Instead, the Secretary of State is given a power to require retention of data by serving a notice on an operator.
128. Secondly, the Secretary of State may only exercise that power if she considers it both necessary and proportionate for one or more of the specific purposes currently listed in section 61(7) of the Act. This enshrines in the statute the essence of the tests propounded by CJEU in *Watson*.
129. Thirdly, although the Claimant relies heavily upon section 87(2)(b) as allowing a notice to require the retention of “all data”, that provision cannot be read in isolation and taken out of its context. The Claimant’s submission overlooks the statutory requirement to satisfy the necessity and proportionality tests. It is difficult to conceive how a retention notice drafted so as to encompass all communications data in the UK could satisfy those tests. In any event, section 87(2) provides that a notice may relate to a “description of data” and not just to “all data”. Furthermore, a notice may relate to a particular operator or to a description of operators. These and the other matters specified in section 87(2) must be read as a whole. Taken together they simply list the elements which may be used when delineating the content and scope of a retention notice so as to satisfy the necessity and proportionality tests in any particular case.
130. Fourthly, although a retention notice may specify the period of time for which data is to be retained (section 87(2)(c)), that period may not exceed 12 months (section 87(3)).
131. Fifthly, before the Secretary of State may serve a retention notice, she must have regard to, among other matters, the factors listed in section 88(1), which comprise the likely benefits of serving the notice, the number of users to which the notice relates, the technical feasibility and costs of complying with the notice and any other effect on the telecommunications operator to be served. In addition, before serving a retention notice the Secretary of State must also take reasonable steps to consult any operator to whom the notice will relate (section 88(2)).
132. Sixthly, by section 87(1)(b) a retention notice may not be given unless the Secretary of State’s decision has been approved by a Judicial Commissioner under section 89. These provisions have not yet been brought into force, but we think it would be quite unrealistic to ignore them at this stage. The Judicial Commissioners had been appointed by October 2017. In para. 53 of his first witness statement, Mr Andrew Scurry (Head of the Investigatory Powers Unit in the Home Office) states that the remaining provisions of Part 4 (including the provisions relating to approval by a Commissioner) will be brought into force when the 2016 Act is amended in response to *Watson* CJEU. It was confirmed by Mr Eadie during the hearing that those amendments are due to be considered by Parliament before the summer recess begins in July 2018 (in line with para. 13 of the letter from the Government Legal Department dated 26 July 2017 and para. 14 of the Defendants’ skeleton).

133. In deciding whether to approve a retention notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the requirements in the proposed notice are necessary and proportionate for one or more of the purposes in section 61(7) (see section 89(1)). In performing this function, a Commissioner must apply the same principles as would be applied by a court in an application for judicial review and ensure that his or her consideration is sufficiently careful so as to comply with the duties in section 2 of the Act. By section 2(2) a Commissioner must have regard to :-

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

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

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

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

The reference in section 2(2)(b) to “sensitive information” includes items subject to legal privilege and any information identifying a source of journalistic information (section 2(5)). By section 2(4) a Commissioner may also have regard to any other consideration relevant to whether the proposed notice is *necessary* for one of the statutory purposes and is *proportionate*, and the requirements of the HRA and of public law.

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

135. In the light of this analysis of the structure and content of Part 4 of the 2016 Act, we do not think it could possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data. The legislation requires a range of factors to be taken into account and imposes controls to ensure that a decision to serve a retention notice satisfies (*inter alia*) the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles.

136. The Claimant sought to rely upon paras. 64-65 of the decision of *Watson DC*, where, because the Defendant had not provided any evidence as to the contents of any retention notice, the Court tested the validity of DRIPA on the assumption that the retention notices that could be issued might be as broad in scope as the statute permits, namely a direction to each service provider to retain all communications data for 12 months. Even if that assumption were to be applied in this case, it is plain from the analysis set out above, that the 2016 Act does not permit the general and indiscriminate retention of communications data. In any event, we would add that the

issue of whether a UK enactment is inconsistent with EU legislation is not to be determined by *evidence* from either party as to how the domestic scheme is operated in practice or might be operated. Instead, the issue is an objective question of law which turns on the proper interpretation of the two pieces of legislation.

137. Ultimately, the overall amount of data which is retained under Part 4 of the 2016 Act will be the outcome of applying a statutory regime which requires the contents of each retention notice to be necessary and proportionate. This rigorous approach required by the 2016 Act will be reinforced when the provisions for judicial scrutiny are brought into force.
138. For all these reasons we reject the Claimant's contention that Part 4 of the 2016 Act is inconsistent with EU law because it provides for the general and indiscriminate retention of traffic and location data.

(4) Entity Data

139. The Claimant submits that the decision in *Watson* CJEU applies to a category of "communications data" referred to as "entity data". The Defendants submit to the contrary and submit that the point is *acte clair*. The Claimant responds that the issue is far from clear and should be referred to the CJEU for determination. The Claimant relies upon the Government's Consultation document issued in November 2017 on its proposed response to *Watson* CJEU, at pages 10-11 of which the Government asks consultees for their opinion on whether its views on this legal issue is correct.
140. This issue turns on the scope of "communications data" as defined in the 2016 Act as compared with the scope of "traffic data" and "location data" as defined in the e-Privacy Directive.
141. As we have said earlier, section 87(1) of the 2016 Act empowers the Secretary of State to serve a retention notice requiring a telecommunications operator to retain "relevant communications data". "Communications data" is defined in section 261(5) as covering two mutually exclusive categories of data, namely "entity data" and "events data", which in either case must satisfy certain additional criteria.
142. For these purposes an "entity" means a person or thing (section 261(7)).
143. Section 261(4) defines "events data" as:

"any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time".
144. Section 261(3) defines "entity data" as:

"any data which –

 - (a) is about –
 - (i) an entity

- (ii) an association between a telecommunications service and an entity, or
 - (iii) an association between any part of a telecommunication system and an entity,
- (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and
- (c) is not events data.”

Thus, para. (c) prevents there being any overlap between events data and entity data. In so far as it may be necessary to allocate data to one or other of these two categories, the language of section 261(3) indicates that it would be sensible to apply the definition of “events data” first.

145. In summary, “events data” comprises data which identifies or describes events taking place on or by means of a telecommunication system where at least one “entity” engages in a specific activity. An example of events data would be the making of a call between two mobile phones and the time and duration of that call. If an item falls within “events data” because it identifies or describes such a communication, it cannot also be treated as “entity data”. Subject to that exclusion, “entity data” comprises data about a person or thing or about associations between such entities. An example of entity data would be the name of a person who owns a particular mobile phone or the number of that phone. For completeness, we note that the definition of “communications data” in section 261(5) read together with subsection (6) excludes “the content” of any communication.
146. Paragraph 2 of the dispositif in *Watson* CJEU decided that Article 15(1) of the e-Privacy Directive precludes national legislation which allows access by competent national authorities to retained “traffic data” and “location data” for the purposes of fighting crime unless the minimum mandatory requirements stipulated by the CJEU are satisfied. As we have said, the hearing before us was confined to that part of the claim which challenges Part 4 of the 2016 Act. The express provisions of Part 4 relate solely to the retention of data. But in *Watson* the CJEU decided (at para. 79) that since a requirement to retain data is only imposed to enable that data to be accessed where necessary by competent authorities, legislation requiring retention necessarily entails provisions for that access and the conditions under which such access may take place. As matters currently stand, access to data retained under Part 4 of the 2016 Act may be authorised under Chapter II of the Regulation of Investigatory Powers Act 2000 (“RIPA 2000”), just as was the case with DRIPA (*Watson* CJEU at paras. 39-43).
147. The terms “traffic data” and “location data” are defined in Article 2 of the e-Privacy Directive. The Defendants submit that the term “events data” in section 261(4) of the 2016 Act encompasses anything falling within “traffic data” or “location data” under that Directive and so the decision in *Watson* CJEU does not apply to the category of “communications data” in that Act, defined as “entity data”.
148. In Article 2 of the e-Privacy Directive: -

“ ‘traffic data’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”

and

“ ‘location data’ means any data processed in an electronic communications networks or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.”

149. We accept the Claimant’s submission that the true interpretation of these provisions is an objective question of law for the Court to determine, and is not affected by the outcome of the Government’s consultation exercise referred to above (cf. para. 39 of the Defendants’ skeleton).
150. The Claimant puts forward what are said to be examples of either “traffic data” or “location data” which cannot fall within the definition of “events data” but do fall within the definition of “entity data” (para. 74(2)(c) of the Claimant’s skeleton). First, it is said that the address or specific location of a fixed line terminal falls within both “location data” and, where no communication is recorded, “entity data”. Secondly, it is said that a billing address and billing details (such as details of a bank account or credit card) fall within both “traffic data” and “entity data”. Similarly, where billing data does not identify or describe an event it is “entity data”. Such data simply describes an “association” with a telecommunications system or part thereof.
151. In paras. 41-42 of their skeleton, the Defendants submit that in so far as the Claimant’s examples fall within the definition of “entity data” they do not fall within the definitions in the e-Privacy Directive of “traffic data” or “location data” and so do not fall within the scope of the CJEU’s decision in *Watson*. We agree.
152. “Traffic data”, as the language suggests, is concerned with the processing of data for the purposes of *conveying* a communication. That definition is extended to include “billing data”, but only data for the billing of such a communication. It does not include billing data in general, which is unrelated to a relevant communication. That is reinforced by recital (27) in the preamble to the e-Privacy Directive, which refers to the moment at which *transmission of a communication* is completed and “traffic data” should then be erased except for billing (see also Article 6). Accordingly, the mere holding of a billing address or bank account details does not fall within the “billing” limb of “traffic data”. The type of billing information which is to do with the billing of the “conveyance of a communication” would include an itemised phone bill, where the time, duration and cost of each call are set out. Plainly, such data identifies or describes an “event” and is not entity data.
153. “Location data” must be data which is processed either “in an electronic communications network” or “by an electronic communications service”. It is insufficient that the data merely (referring to the second part of the definition) indicates “the geographic position of the terminal equipment of a user of a publicly available electronic communications service”. Thus, where the address and specific location of a fixed line terminal is simply *held* as a data by a service provider without being *processed* either in a communications network or by a communications service, that data is not “location data” for the purposes of the e-Privacy Directive.

154. Accordingly, we conclude that the definition of “events data” under the 2016 Act embraces both “location data” and “traffic data” in the e-Privacy Directive and so “entity data” under the 2016 Act does not fall within the scope of paragraph 2 of the dispositif in *Watson* CJEU.

155. Because we are satisfied that this is *acte clair*, a reference to the CJEU would be inappropriate.

(5) Whether there is a “seriousness” threshold for all retention objectives

156. The CJEU has decided that the derogation from the principle of confidentiality permitted by Article 15(1) of the e-Privacy Directive for the prevention, investigation, detection and prosecution of criminal offences is limited to the objective of fighting *serious* crime (paras. 108 and 115 of *Watson* CJEU). The Claimant argues that a threshold of “seriousness” should also be applied to the other objectives referred to in Article 15(1) and hence the statutory purposes in the 2016 Act for which retention notices may be served.

157. In *Watson* DC the Claimants mounted essentially the same argument in relation to the similar statutory purposes laid down in DRIPA, relying upon the decision of the CJEU in the *Digital Rights Ireland* case at para. 60. The Court of Appeal rejected that argument in 2015, at para. 85:-

“Ms Rose now submits instead that [para. 60] gives rise to a mandatory requirement of compliance with a high threshold of seriousness for any justification for a provision granting access to retained data. She submits that whatever the purpose may be, it must meet a defined threshold of seriousness. While we would certainly accept that the more serious the interference with fundamental rights, the more serious the justification must be, we are unable to accept that the CJEU was here intending to lay down a mandatory requirement which could justify a national court in holding national legislation invalid without a detailed consideration of the legislative scheme under challenge. The principle contended for is insufficiently specific to lead to such a result.”

158. The Court of Appeal’s conclusion remains undisturbed by anything said in the CJEU’s decision. We agree with the Defendants that the fact that national legislation such as the 2016 Act does not impose a “seriousness” threshold on a permissible objective for requiring the retention of data (or access thereto) does not render that legislation incompatible with EU law.

159. It is important to understand this issue in its proper legal context. What this issue addresses is the question: what objectives are capable of providing a legitimate aim for an interference with a fundamental right? Just because something is capable of providing a legitimate aim does not mean that the interference will be justified. Other questions will still have to be addressed, for example does the interference satisfy the requirements of proportionality?

160. It is easy to see why the CJEU thought it necessary to restrict the “fighting crime” objective to serious criminal offending. Criminal offences cover an enormous spectrum, ranging from (for example) relatively minor regulatory infringements to

homicide and terrorist acts. Many criminal offences are insufficiently serious to be capable of justifying an interference with rights under Articles 7, 8 and 11 of the Charter of Fundamental Rights.

161. The same considerations do not apply to the other objectives which EU law allows to be the subject of requirements for the retention of and access to communications data. Objectives concerned with, for example, the interests of national security and public safety and the investigation of miscarriages of justice have sufficient intrinsic importance to be capable of justifying an interference with Articles 7, 8 and 11, without the need to superimpose any “seriousness” threshold. The degree of seriousness involved in any situation falling within any of these cases is adequately dealt with through the application of the necessity and proportionality tests in section 87(1) and other parts of the 2016 Act. The addition of a “seriousness” threshold would add nothing of substance to the legislative scheme. Indeed, Mr Jaffey acknowledged that a threat to national security would readily cross such a threshold in any event.
162. The Claimant sought to add this issue to its list of matters to be referred to the CJEU, but for the reasons we have given the Claimant’s contention must be rejected. We consider the matter to be *acte clair*.

(6) Retention of data within the EU

163. Paragraph 2 of the dispositif in *Watson* CJEU stated that Article 15(1) of the e-Privacy Directive precluded access to retained traffic and location data for the purposes of fighting crime, in the absence of a requirement “that the data ... should be retained within the European Union”.
164. As originally formulated in the Statement of Facts and Grounds, the issue was whether that requirement is absolute in effect or whether instead it may be relaxed so as to allow retained data to be passed outside the EU subject to compliance with safeguards, and if so what safeguards. However, in his submissions on behalf of the Claimant, we understood Mr Jaffey to have accepted that the requirement is not absolute. Both parties agree that the subject is not *acte clair*. The Claimant asks us to order a reference of the issue to the CJEU. The Defendants resist that application.
165. The Defendants submit that the CJEU could not have intended to lay down in *Watson* a requirement amounting to an absolute embargo on the transfer of data out of the EU, not least because of Article 25 of the Data Protection Directive (Directive 95/46/EC). The Defendants submit that there is considerable uncertainty as to the effect of the CJEU’s decision, but that the relevant issues have already been raised in the reference made by the Investigatory Powers Tribunal in *Privacy International*.
166. In paras. 65-68 of its judgment the IPT explained its understanding of the relevant case law and raised the issue of whether there is an absolute bar on transfer of data outside the EU, or whether instead it would suffice for there to be an independent review of the kind described in para. 123 of *Watson* CJEU. The same issues are summarised in paras. 52-55 of the order for a reference. Question 2 in that order fairly and squarely raises the issue as to how, and the extent to which, the requirement for retention of retained data within the EU applies to the acquisition and use by the Security Intelligence Agencies of “bulk communications data” pursuant to section 94 of the 1984 Act.

167. Mr Jaffey submits that the reference by the IPT is inadequate for the purposes of the present litigation because the Government will contend that, by virtue of Article 4 of the TEU, the powers exercisable under section 94 fall outside the scope of EU law, including the e-Privacy Directive. He says that the arguments in the *Privacy International* case are focused on the ability of the UK to *acquire* bulk data for national security purposes. If the CJEU were to determine those issues in the Government's favour under question 1 then there is a real risk that the Court will decide not to deal with question 2.
168. We are unimpressed by the Claimant's submissions on this point. Although the present challenge is concerned with the retention of, rather than acquisition of or access to, data, *Watson* CJEU has established that the two are intimately connected. The purpose of retaining data is to enable any necessary and authorised access to take place.
169. The powers under section 94 of the 1984 Act are exercisable if considered by the Secretary of State (*inter alia*) "to be necessary in the interests of national security". But Article 4(2) of the TEU requires the EU to respect "the essential state functions" of member states as regards not only "safeguarding national security" but also "maintaining law and order". Moreover, there is a degree of overlap between national security issues and fighting certain types of serious crime. As we have said earlier when addressing the issue of national security, we agree with Mr Eadie that the IPT's reference raises profound issues such that it is likely that that CJEU will give full consideration to both questions in the reference. In our judgement it would be inappropriate to order a further reference at this stage to deal with "the retention of data within the EU" issue.
170. We are reinforced in that conclusion by the views expressed by the Court of Appeal in *Watson* CA 2018 at paras. 14-19. The Court referred to the need for the CJEU to clarify whether it intended in *Watson* to lay down an absolute requirement and, if not, to clarify what safeguards are required. Lord Lloyd-Jones expressed the hope that these uncertainties in EU law will be resolved by the CJEU (para. 19). The Court decided that in relation to DRIPA it should not make a definitive statement on the issue in the form of a declaration. Instead, the Court proceeded on the basis that the uncertainties, which affect the 2016 Act in much the same way as DRIPA, should be resolved in the reference which had already been made by the IPT. We have reached the same conclusion.
171. Mr Jaffey also sought to persuade us to order a reference because of three specific factors relied upon by Court in para. 122 of *Watson* CJEU as justifying the need for data to be retained within the EU, namely (1) the quantity of data retained, (2) the sensitivity of data and (3) the risk of unlawful access. He suggested that consideration needed to be given to a requirement for the retention of whole data sets. Mr Eadie rightly submitted that points (2) and (3) are common to the use of the powers under section 94 of the 1984 Act and Part 4 of the 2016 Act. We also accept his submission that in the light of the Opinion issued by CJEU in *Opinion 1/15* EU:C:2017:592, the "quantity of data" which may be retained does not give rise to any freestanding issues in the present litigation so as to justify the making of a reference.
172. Accordingly, this part of the claim for judicial review must be stayed pending the CJEU's decision in the reference in the *Privacy International* case.

(7) Notification to Persons Affected

173. The CJEU has decided that, where access to retained data is granted, the competent authority must notify the persons affected under domestic law procedures as soon as that notification is no longer liable to jeopardise the investigations it is undertaking (para. 121 of *Watson* CJEU). However, as the Court of Appeal pointed out in *Watson* CA 2018 (at para. 21) that statement did not form part of the Court's dispositif. The Claimant submitted that we should refer this issue to the CJEU for clarification.
174. The Claimant submits that without notification a person affected by his or her data being accessed will be unable in practice to use any available remedy. Mr Jaffey also points out that, whereas in a criminal trial a defendant who is so affected will receive notification through the formal process of disclosure, no process of notification is provided for those who are not accused of, or implicated in, criminal conduct.
175. We accept the submission of Mr Eadie that the decision in *Watson* CJEU was confined to notification in the event of data being *accessed*. There is no requirement for notification as a consequence of the Secretary of State requiring data to be *retained*. Ultimately, we did not understand the Claimant to argue otherwise. For obvious reasons, it would be wholly impractical to have a general legal requirement of notification for all retained data. Furthermore, the evidence before us suggests that most of the data retained is not accessed before it is destroyed. It is simply stored so that any access may be obtained to specific data where that is properly justified and authorised. Accordingly, it is wholly unsurprising that the CJEU referred to notification solely in the context of access and not retention.
176. The hearing before us was only concerned with the Claimant's challenge to Part 4 of the 2016 Act, and so the "access" point is relevant only as a corollary of retention. We note that in its Consultation Document issued in November 2017 the Government has sought comments on notification requirements to be considered in relation to Part 3 of the 2016 Act as part of its proposals to amend that legislation.
177. In *Watson* CA 2018 the Court of Appeal refused (at para. 21) to make a declaration that DRIPA was incompatible with EU law through failing to provide notification of access having been granted to data, in order to reflect para. 121 of the CJEU's judgment. One of the main reasons for the Court's decision was the fact that the CJEU will consider the relevant issues in the reference from the IPT in the *Privacy International* case (see paras. 62-64 of the IPT's judgment).
178. Plainly, the Court of Appeal considered that there were uncertainties in relation to para. 121 of the CJEU's judgment which precluded it from making any statement about the possible application of that paragraph to DRIPA. It is also plain that, in view of the reference that had been made by the IPT, the Court of Appeal did not consider that any further reference to the CJEU was appropriate in order for the necessary clarification to be obtained. We do not consider that the 2016 Act gives rise to any materially different issues which could justify the making of a further reference to the CJEU on this aspect.
179. There remain the Defendant's submissions that the 2016 Act contains specific provisions which are sufficient to satisfy any notification requirement resulting from the decision in *Watson* CJEU. They rely upon section 231 of the Act, which will require the Investigatory Powers Commissioner to notify a person of a "serious error"

(i.e. one that has caused significant harm or prejudice to that person) if he considers it to be in the public interest to do so. In addition, section 243 will amend RIPA 2000 so as to widen the powers of the IPT to hear claims from affected persons. The Claimant makes several criticisms of the adequacy of these provisions.

180. We do not think it appropriate at this stage to resolve the competing arguments concerning the safeguards in the 2016 Act and in particular to decide whether the Defendants' argument that the 2016 Act contains sufficient protection for parties whose data is accessed is correct. First, the provisions relied upon by the Defendants had not been brought into force at the date of the hearing before us in February 2018. However, in later written submissions the Defendants have drawn our attention to the fact that:

(1) The amendments to section 65 of RIPA 2000 enacted by section 243 of the IPA, insofar they give the Investigatory Powers Tribunal jurisdiction over the giving of retention notices and conduct under a retention notice, and insofar as they give the Tribunal power to quash or cancel a retention notice, came into force on 12 March 2018 (see regs. 2(c)(i)(aa) and 2(c)(iv) of the Investigatory Powers Act 2016 (Commencement No.4 and Transitional and Saving Provisions) Regulations 2018, SI 2018/341).

(2) The Tribunal already has jurisdiction to consider conduct in relation to access to communications data: see section 65(1)(c) of RIPA 2000 (such conduct presently falls within Part I of RIPA, not the IPA, pending the coming into force of Part 3 of the IPA).

181. Secondly, the Government has yet to announce its conclusions in relation to its consultation on this subject. As a matter of legal principle, the Government cannot have reached a concluded view on the adequacy of the measures it has proposed.

182. Thirdly, it would be undesirable for this Court to express a conclusion on this matter before the CJEU has given its decision in the reference from the IPT.

183. This part of this claim will also be stayed pending the CJEU's decision in the reference in the *Privacy International* case.

(8) Legal professional privilege

184. The Claimant submitted that this issue arose because the Defendants were proceeding on a legally incorrect basis, namely that the term "communications data" in the 2016 Act could not include data which is the subject of legal professional privilege. Of course, that is an entirely separate question from any issue as to whether Part 4 of the 2016 Act is incompatible with EU law by failing to provide sufficient protection for data protected by this privilege. Mr Eadie stated that the Defendants do not maintain that communications data cannot include legally privileged material. On that basis Mr Jaffey told the court that there are no issues under this heading for us to resolve at this stage.

(9) Codes of Practice

185. The Claimant submits that codes of practice issued under the 2016 Act may not be taken into account when determining whether that legislation complies with requirements of EU law for mandatory minimum safeguards as laid down in *Watson* CJEU, or to satisfy Articles 7, 8 and 11 of the Charter of Fundamental Rights. We recognise why this issue is of potential importance to the Government as there is a longstanding principle in human rights law, which has been developed by the European Court of Human Rights since the 1970s, that the requirement that an interference with a Convention right must be “in accordance with law” may be satisfied by having in place “soft law” such as a code of practice and does not necessarily require there to be legislation in place. However, Mr Eadie confirmed to the Court that the Defendants do not in fact rely upon the content of any code of practice in order to resist the challenges upon which the court is being asked to adjudicate at this stage. We therefore decline to consider or determine the hypothetical arguments presented by the parties under this heading.

Conclusion

186. For the reasons we have given this claim for judicial review succeeds in part, because Part 4 of the Investigatory Powers Act 2016 is incompatible with fundamental rights in EU law in that in the area of criminal justice:
- (1) access to retained data is not limited to the purpose of combating “serious crime”; and
 - (2) access to retained data is not subject to prior review by a court or an independent administrative body.
187. We have concluded that the legislation must be amended within a reasonable time and that a reasonable time would be 1 November 2018, which is just over 6 months from the date of this judgment. We have also concluded that the appropriate remedy is a declaration to reflect our judgment.
188. Finally we would like to express our gratitude to all counsel and those instructing them for their assistance in this important case.