IN THE HIGH COURT OF JUSTICE **Claim No: CO/1052/2017**

QUEEN'S BENCH DIVISION

ADMINISTRATIVE COURT

BETWEEN:

THE QUEEN

on the application of

LIBERTY

Claimant

- and -

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(2) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

Defendants

CLAIMANT'S SKELETON ARGUMENT FOR HEARING ON 27–28 FEBRUARY 2018

Time Estimate for Hearing: 2 days

Suggested Pre-Reading (1 day):

- **Liberty's Statement of Facts and Grounds ("SFG")**
- **Defendants' Detailed Grounds of Resistance ("DGR")**
- **First Witness Statement of Silkie Jo Ellen Carlo dated 28 February 2017 ("Carlo 1"), First Witness Statement of Andrew Scurry (undated and unsigned) ("Scurry 1"), First and Second Witness Statements of Corey Lynn Stoughton dated 15 January 2018 and 8 February 2018 ("Stoughton 1" and "Stoughton 2"), First Witness Statement of Graeme Biggar dated 31 January 2018 ("Biggar 1")**
- **Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and R (Watson) v Secretary of State for the Home Department* ECLI:EU:C:2016:970 ("*Watson CJEU*")**
- ***Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70 ("*Watson CA*")**
- ***Privacy International v Secretary of State for the Foreign and Commonwealth Office* [2017] UKIPTrib IPT_15_110_CH and Order for Reference made by the Investigatory Powers Tribunal**

Further references in this Skeleton Argument appear as follows:

- **Witness statements appear in the form "Name ¶*x*"**

- **Defendants' Summary Grounds of Resistance ("SGR")**
- **Order of Jeremy Baker J granting permission dated14 July 2017 ("Permission Order")**

This Skeleton Argument will be replaced by a version updated to include bundle references once the bundle is agreed between the parties.

A SUMMARY

1. The Claimant ("**Liberty**") challenges the compatibility of the Investigatory Powers Act 2016 ("**IPA**") with European Union ("**EU**") law and the European Convention on Human Rights ("**ECHR**"). It contends *inter alia* that the decision of the Court of Justice of the EU in *R (Watson) v Secretary of State for the Home Department* ("***Watson CJEU***")[1] establishes that Part 4 of the IPA is incompatible with EU law.

2. Part 4 authorises retention of "communications data" (broadly, all information about electronic communications except their content). Retention of and access to communications data is a significant inference with rights under Articles 7 and 8 of the EU Charter of Fundamental Rights ("**CFR**"), as is common ground,[2] and with Article 11 of the CFR. Such retention and access is also a breach of Article 5 of the e-Privacy Directive, requiring justification under Article 15 of the same Directive.[3]

3. *Watson CJEU* confirms that EU law (i) prohibits indiscriminate and general retention of and access to communications data and (ii) requires retention/access regimes to contain specified mandatory minimum safeguards (for example, prior independent authorisation of access to retained communications data).

4. The IPA received Royal Assent on 29 November 2016. Part 4 was brought into force (without the key safeguard of prior judicial approval of a retention notice) on 30 December 2016[4] and substantially re-enacts the Data Retention and Investigatory Powers Act 2014 ("**DRIPA**"). The Court of Appeal recently confirmed that DRIPA, which has been repealed, was incompatible with EU law: *Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70 ("***Watson CA***").

---

1 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and R (Watson) v Secretary of State for the Home Department* ECLI:EU:C:2016:970.

2 SFG ¶¶33–39; DGR ¶¶10–13. The DGR fail to respond on Article 11.

3 SFG ¶85. The DGR fail to respond.

4 See Investigatory Powers Act 2016 (Commencement No 1 and Transitional Provisions) Regulations 2016/1233 reg 2. Important safeguards — ss 87(1)(b), 89 and 91, which require review by judicial commissioners of retention notices, and s 90(1)–(12), which permit a telecommunications operator to refer a retention notice back to the Secretary of State — still have not been commenced more than a year after the balance of Part 4 commenced.

5. The Defendants having refused to respond substantively to pre-action correspondence,[5] Liberty issued its claim on 28 February 2017. On 14 June 2017, Jeremy Baker J rejected the Defendants' submissions[6] that the claim should be dismissed as premature or futile. He gave Liberty permission to challenge Part 4, stayed the rest of the claim, and required the Defendants to state by 5 July whether they conceded the Part 4 challenge.[7]

6. In **SGR**, filed 6 April 2017, the Defendants had said at **¶5**: "*the Defendants do not accept that the claim, or any particular part of it, is arguable*" and that "*Part 4 of the Act will need to be carefully considered (and potentially amended)*" (emphasis added).[8] But on 7 July 2017, the Defendants conceded that (see also **DGR ¶5**):

> "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."

7. They conceded that declarations should be made accordingly in this claim. (The concession is without prejudice to whether EU law applies "*in a national security context*".) It is therefore common ground that Part 4 is in some respects incompatible with the EU law requirements laid down *Watson CJEU*.

8. Notwithstanding that concession, Part 4 has not been amended. Unlawful retention of and access to communications data continues. Further, other provisions of Part 4 that Liberty impugns as incompatible are undefended in the DGR.

9. At this hearing, the Court is invited to determine three issues:

---

5 BM/GLD (27 January 2017); GLD/BM (13 January 2017); BM/GLD (21 February 2017); GLD/BM (23 February 2012).

6 SGR ¶¶1, 4.

7 Permission Order ¶¶1–2, 4.

8 It is difficult to understand on what basis this submission was made. On the same day, 6 April 2017, the First Defendant wrote to Tom Watson MP and stated that DRIPA (which Part 4 of the IPA replicates) was "*inconsistent with EU law because it did not contain prior judicial approval or independent administrative authorisation of applications for retained communications data, and the crime purpose for which data could be retained or acquired was not restricted to serious crime*".

(1) **Disapplication:** Liberty submits that the Court should disapply Part 4 insofar as it is conceded to be in compatible with EU law or undefended. This is necessary to give full effect to EU law and provide an effective remedy. It is the course suggested by recent Supreme Court authority. The order for disapplication should be suspended until 31 July 2018, as the Defendants previously suggested.[9] This will give Parliament a reasonable (but time-limited) opportunity to introduce legislation compatible with EU law. This was the course taken by the Divisional Court in *Watson*. The Defendants oppose disapplication: **DGR ¶¶7(d), 137**.

(2) **Protection of legal privilege:** Liberty submits that the Defendants are making a clear error of law by proceeding on the basis that communications data can never be subject to legal professional privilege, and therefore not according any of the requirements that must be observed when conducting secret electronic surveillance of communications data. This is (i) wrong as a matter of English law and (ii) contrary to the government's own prior concessions in recent litigation in the Investigatory Powers Tribunal ("**IPT**"). Liberty seeks declaratory relief.

(3) **CJEU Reference:** Liberty submits that, in light of *Watson CA*, handed down on 30 January 2018, this Court should: (a) refer to the CJEU questions on interpretation and application of the *Watson* mandatory minimum safeguards that the Defendants do not concede have been breached, (ii) the application of EU law in the "*national security context*", and (iii) the protection of lawyer–client communications where communications data is retained/accessed; and (b) invite the CJEU to expedite the reference.

Liberty has suggested since August 2017 that a reference would be required.[10] The Defendants appear to have anticipated, prior to *Watson CA*, that the Court could (mostly) decide the compatibility of Part 4 with EU law without a further reference (**DGR ¶108**). However, *Watson CA* holds that the existence and content of certain *Watson* mandatory minimum safeguards remains unclear as a matter of EU law, in some cases accepting the First Defendant's submissions to that effect. The Investigatory Powers Tribunal has also referred related but distinct questions

9 GLD/BM (28 July 2017) ¶13.

10 Claimant's Submissions in Support of a Costs Capping Order (7 August 2017) ¶9(1).

on different legislation, but this will not resolve all existing uncertainties (and may resolve very few, if any, of relevance, as explained below).

10. The Defendants also seek to re-litigate questions of prematurity and futility that Jeremy Baker J rejected when Liberty was given permission to pursue its Part 4 challenge. The Defendants' submissions should again be rejected.

11. Part 4 is in force – and has been for 13 months. The Defendants concede that it has always been, and is, incompatible with directly effective EU law. It is therefore unlawful, under the European Communities Act 1972, to apply it. Despite this, retention of and access to communications data under Part 4 continues. In those circumstances, the claim for disapplication, based on all pleaded *Watson* requirements, is neither premature nor futile.

B THE INVASIVENESS OF RETENTION OF AND ACCESS TO COMMUNICATIONS DATA

12. Liberty's evidence establishes that the retention of and access to communications data involves a significant intrusion into rights to private life, protection of personal data and freedom of expression, under CFR Articles 7, 8 and 11 and Articles 5, 6, 8(1), (2), (3) and (4) and 9 of Directive 2002/58 (the "**e-Privacy Directive**"). This evidence is almost entirely uncontested.

13. **Carlo 1**, served by Liberty on 28 February 2017, is not disputed. Ms Carlo's evidence on communications data (**Carlo 1 ¶¶19–44**) is in summary that:

    (1) "communications data" includes in practice data such as the sender, recipient, time, duration, type, method, pattern or fact of a communication (such as a telephone call, email or text message), extends to data concerning internet use, such as websites visited,[11] names, physical addresses and billing data, and can be used to identify a person's mobile phone or computer (**Carlo 1 ¶21**);

    (2) communications data can be of <u>more</u> use in building a picture of a person's life than content, because it can be easier than other data to handle, filter and analyse

[11] That "communications data" extends (at least) to websites visited is now common ground: **Biggar 1 ¶11**.

(as it is mostly numeric and can easily be subject to automated processing and analysis) (**Carlo 1 ¶27**);

(3) a single item of communications data can reveal very important and sensitive facts (for example, a record of a call by a senior civil servant to a journalist shortly before a story on a major leak is published) (**Carlo 1 ¶29**);

(4) retention of and access to communications data, in Liberty's experience, discourages whistle-blowers and those who provide information to journalists or watchdog organisations (**Carlo 1 ¶¶42–43**).

14. **Stoughton 1** is also largely uncontested.[12] The key points in Ms Stoughton's evidence (none of which **Biggar 1** suggests to be incorrect as a matter of fact) are that:

(1) "*Communications data produces a deep and comprehensive understanding of a person's private life, revealing aspects of her interests, identity, relationships, movements and activities*" (**Stoughton 1 ¶7**). Internet connection records ("**ICRs**") and mobile telephone location data illustrate this:

(a) ICRs reveal the newspapers you read online, where you shop, what interest-based forums you join, what online dating sites you use, whether, when and where you access pornography, or whether you visit websites for those with HIV, other medical conditions or for those considering abortion (**Stoughton 1 ¶10**).

(b) Mobile telephone location data precisely and frequently records a user's whereabouts relative to mobile phone towers, because modern mobile devices connect automatically to the network and cell sites are increasingly ubiquitous and accurate in pinpointing the source of the signal (**Stoughton 1 ¶¶15–27**). This data can be used to generate a detailed picture of where a person was and was going and to identify other intimate details of their

[12] The Defendants' further witness statement of Mr Biggar **(Biggar 1)** suggests that Ms Stoughton "*misunderstands*" the effect of changes to the text of the draft code of practice and is incorrect in relation to whether data about what apps a person subscribes to would be communications data](**Biggar 1 ¶¶10, 18**). **Stoughton 2** ¶19-23 respond to these points

lives, for example, that they had visited a doctor of a particular kind, religious service or a lawyer (**Stoughton 1 ¶¶23–24**).

15. **Passmore 1**[13] explains the effects of retention of communications data in the context of legal professional privilege. He explains in particular that:

    (1) He considers that the use of surveillance powers "*is beginning to cause a 'chilling effect' on the willingness of some clients to engage in privileged communications*" (**Passmore 1 ¶13**); and

    (2) Some of his clients have changed their behaviour in particular in the last 10 years due to the possibility of the use of secret surveillance powers, for example, using the app "WhatsApp" (which is encrypted) for messaging, and client requests for Mr Passmore to attend their houses without his mobile telephone turned on (**Passmore 1 ¶23**).

    Biggar 1 does not respond to Mr Passmore's statement. Mr Passmore's evidence is thus entirely uncontested.

16. Access to communications data may be, in particular cases, useful for preventing and detecting crime, national security or other purposes. Liberty's EU law challenge to Part 4 does not, however, turn on the usefulness of communications data or the appropriateness of a regime permitting targeted access with proper safeguards. The question is one of law: whether the regime for retention has the safeguards that EU law requires, as identified in *Watson CJEU*. Intrusive capabilities must be balanced by appropriate limits and safeguards.

C THE LAW

17. Liberty's claim is based on the infringement of the following rights:

    (1) Articles 7 (respect for family and private life), 8 (protection of personal data) and 11 (freedom of expression and information) under the EU Charter of

[13] Mr Passmore is the author of Colin Passmore, *Privilege* (3rd ed, 2013), commonly known within the legal profession as "*Passmore on Privilege*".

Fundamental Rights ("**CFR**"), from which derogation is governed by Article 52 **(SFG ¶85)**; and

(2) the rights, to confidentiality and integrity of personal data, under Articles 5, 6, 8(1), (2), (3) and (4) and 9 the e-Privacy Directive, from which derogation is governed by Article 15(1) **(SFG ¶86)**.

18. The above principles are almost entirely[14] common ground (**SFG ¶¶ ; DGR ¶¶9–22**). The dispute is as to:

(1) the consequences of accepted or undefended incompatibility with EU law, in particular, whether a suspended order for disapplication should be made; and

(2) the correct interpretation of *Watson CJEU* and whether this Court should refer those issues to the CJEU.

D THE COMMUNICATIONS DATA RETENTION AND ACCESS REGIME IN PART 4

19. Part 4 (read with Part 3) permits the Secretary of State to issue a "**retention notice**" under s 87. A retention notice requires (one or many) telecommunications operators to retain (potentially all) "*relevant communications data*" of any description. This may include all communications data and as yet non-existent communications data (s 87(2)). Retention may be for at most 12 months from specified dates (s 87(3)).

20. The notice must be considered necessary and proportionate for any of a wide range of purposes or interests:

"(a) in the interests of national security,

(b) for the purpose of preventing or detecting crime 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,

[14] The Defendants fail to respond to Liberty's argument that CFR Article 11 is also engaged.

(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,

(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. Further details of Part 4 are at **SFG ¶¶18(5) and 170** and **DGR ¶¶74–79**. As DGR ¶75 n 15 notes, the safeguard of approval by a Judicial Commissioner of a retention notice is not yet in force. The provisions of Part 4 are considered below as necessary.

E PART 4 SHOULD BE DISAPPLIED

22. The Court is invited to disapply Part 4 in the respects that are (i) conceded by the Defendants to be incompatible with EU law or (ii) not now defended.

23. Liberty accepts that the order for disapplication should, in the exercise of the Court's discretion and consistently with previous case law, be suspended to allow a reasonable period (say, until 31 July 2018, which the Defendants previously suggested)[15] for the IPA to be amended.

(1) Conceded and undefended incompatibilities

24. For the reasons below, in light of the concessions made and the Defendants' failure to defend certain provisions of Part 4, the Court should disapply Part 4 insofar as:

[15] GLD/BM (28 July 2017) ¶13.

(1) the purpose of retention of and access to communications data relating to prevention/detection of crime is not limited to preventing and detecting serious crime;

(2) retention of, and access to, retained data are both not subject to prior review by a court or independent administrative body;

(3) retention of and access to communications data is permitted at all for the purposes of:

(a) protecting public health;

(b) assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(c) exercising functions relating to (i) the regulation of financial services and markets, or (ii) financial stability.

(a) Retention and access only for preventing/detecting serious crime in the area of crime prevention and independent authorisation of retention of and access to communications data

25. The Defendants concede that Part 4 is incompatible with EU law, save in "*the national security context*", in two respects (**DGR ¶5**):

> "(i) 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 (ii) access to retained data is not subject to prior review by a court or independent administrative body." [emphasis added]

They concede that Liberty is entitled to declaratory relief on these two aspects.

26. In fact, the concession goes further as to purpose. **DGR ¶85(f)(i)** states that it is proposed to "*impose a 'serious crime' threshold in relation to the retention and acquisition of events data for criminal purposes (in response to §102 of the Watson judgment)*" (emphasis added). Accordingly, the Defendants accept that *Watson CJEU* requires that both retention of and access to/use of communications data in the area of criminal investigations must be restricted to the purpose of preventing/detecting only

serious crime. Liberty put the issue of retention squarely to the Defendants in August 2017.[16] The Defendants' response made clear that the unlawfulness of retention, too, is conceded.[17]

27. In addition, *Watson CJEU* suggests that independent prior authorisation of the retention of communications data, as well as of access to it.[18] The provision in Part 4 for Judicial Commissioner approval of retention notices (s 87(1)(b)) remains un-commenced.[19] This is therefore a clear further incompatibility. The contrary is unarguable. The Court is invited to so declare.

(b) Insufficiently serious purposes in s 61(7) to justify retention of and access to communications data

28. In **SFG ¶¶91–92** and **171(1)**, Liberty pleaded that Part 4 was incompatible with EU law insofar as it was not limited to the purpose of fighting serious crime or (alternatively) "*to serious threats to all of the interests listed in s 61(7) … so in consequence it allows the issue of a warrant for purposes that are not capable of justifying an interference with Article 7 and 8 rights*".[20] The Defendants do not in **DGR ¶¶85(f)(ii), 102(a)(iii)** or **111(c)** (or elsewhere) defend as justifiable purposes for retention and access defined as widely as:

(1) "*protecting public health*" (s 61(7)(e));

(2) "*assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department*" (s 61(7)(e)); or

(3) "*exercising functions relating to — (i) the regulation of financial services and markets, or (ii) financial stability*" (s 61(7)(j)).

---

16 BM/GLD (2 August 2017) ¶12(1).

17 GLD/BM (29 August 2017) ¶11, referring to the fact that the Defendants' 29 July letter had referred to changes being necessary also to the purposes for which retention is permitted (see GLD/BM (29 July 2017) ¶8(b).

18 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [23], [114].

19 Westlaw, Investigatory Powers Act Overview Document (7 February 2017).

20 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [102], [115].

The Defendants instead propose to remove them (**Scurry 1 ¶109**). **DGR ¶102(a)(iii)** concedes this proposal is made "[i]*n light of the judgment in Watson*". **DGR ¶111(c)** appears to accept that these purposes (as framed) are not sufficiently serious to justify retention of and access to communications data.[21]

29. So, Liberty has pleaded and explained why these provisions are incompatible with EU law. The Defendants appear to agree and certainly do not suggest otherwise.

30. The Defendants assert in correspondence that they did not seek to justify retention for these purposes "*as a pragmatic approach to matters that are academic*", given that "*they are proposed to be removed in any event as part of the consultation*".[22] But this issue is not academic: Part 4 authorises retention of and access to communications data now for these purposes. It has done so for over a year. Neither **Scurry 1** nor **Biggar 1** suggests that retention does not occur for these purposes. Further, as explained in paragraph 42 below, the proposal for their removal does not mean they will be removed. Parliament makes the final decision.

(2) Disapplication is required by EU law

(a) Disapplication of Part 4 is required insofar as incompatible with EU law

31. A national court of an EU member state must give "full effect" to EU law, including by (1) disapplying national provisions that are inconsistent with EU law and (2) according an effective remedy when EU law rights have been infringed under CFR Article 47.

32. The CJEU's decision in *Taricco* conveniently states the principle that, where national provisions do not satisfy the requirements of EU law, a national court:[23]

> "would have to ensure that EU law is given full effect, if need be by disapplying those provisions and thereby neutralising the [failure to satisfy EU law], without having to request

---

21 It says relevantly (emphasis added): "*The remaining purposes (to the extent that they are not proposed to be removed in any case as part of the Consultation)* [referring to ss 61(7)(e), (f) and (j)] *are in themselves plainly of sufficient seriousness to justify a proportionate interference with Article 7 and 8 rights.*"

22 GLD/Bhatt Murphy (18 January 2018).

23 Case C-105/14 *Taricco* ECLI:EU:C:2015:555 [49] (emphasis added).

or await the prior repeal of those articles by way of legislation or any other constitutional procedure …"

33. As the CJEU said in *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs*, where a Directive lays down unconditional and sufficiently precise requirements but national provisions cannot be interpreted consistently with the Directive, a national court "*must disapply the rules of national law which are incompatible with the directive concerned*".[24]

34. The provisions of the CFR and e-Privacy Directive on which Liberty relies are respectively primary EU law and a directive that lays down unconditional and sufficiently precise requirements to be directly effective.

35. That is shown by the approach of the Divisional Court in *Watson*, which considered materially identical provisions[25] and made a suspended order for disapplication of DRIPA insofar as it had been found to be incompatible with the EU law now further elaborated in *Watson CJEU*. There, the Divisional Court:

    (1) accepted that the Supreme Court decision in *ClientEarth*[26] where a mandatory order was made requiring production of air quality plans to end non-compliance with EU law, "*does not lay down a rule that disapplication or mandatory relief, even with a reasonable time for compliance, must always be the appropriate remedy*"; but

    (2) nonetheless regarded that decision as "*giv*[ing] *a steer which in our view cannot be ignored*".

36. The Defendants did not, in the Court of Appeal, challenge the Divisional Court's orders on the basis that, in principle, no order for disapplication should have been made.

---

[24] Case C-404/13 *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* ECLI:EU:C:2014:2382 [54].

[25] See generally *R (Davis & Watson) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin), [2016] 1 CMLR 13 [39] (Bean LJ).

[26] *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* [2015] UKSC 28, [2015] 3 CMLR 15 [30] (Lord Carnwath for the Court). See also at [28]: "*regardless of any action taken by the Commission, enforcement is the responsibility of the national courts*". Lord Carnwath also said at [31] the possibility that "*where a responsible public authority is in admitted breach of a legal obligation, but is willing to take appropriate steps to comply, the court may think it right to accept a suitable undertaking, rather than impose a mandatory order*".

37. In *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs*, Lord Carnwath (giving the judgment of the Supreme Court) rejected the submission that the Court should not order compliance with EU law where the Secretary of State stated an intention to comply.[27] He said:[28]

> "without doubting the good faith of the Secretary of State's intentions, we would in my view be failing in our duty if we simply accepted her assurances without any legal underpinning".

38. A (suspended) order for disapplication has utility: it requires amendment by a certain date. It therefore ensures an effective remedy for the admitted breaches of Articles 7 and 8 (and presumably Article 11) of the CFR.

(b) The Defendants' arguments against disapplication should be rejected

39. The **DGR** say only this on disapplication (at **¶137**):

> "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."

(DGR ¶7(d) asserts there is "*no need for any formal relief*" and "*good reason for the Court not to seek to disapply the current provisions under Part 4*".)

40. The Defendants' position is therefore that the Court should not disapply Part 4 insofar as it is conceded to be incompatible or it is undefended because amendments have been <u>proposed</u> and may in time be <u>considered</u> by Parliament.

41. This provides no basis, let alone "good reason", for an argument that the Court should not disapply Part 4 given that:

    (1) Member State courts must, as a matter of directly applicable EU law, give EU law full effect, including by disapplying incompatible provisions of national law; and

---

[27] *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* [2015] UKSC 28, [2015] 3 CMLR 15 [23], [30]–[31].

[28] *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* [2015] UKSC 28, [2015] 3 CMLR 15 [30].

(2) Assurances from government, even in circumstances where it is within the gift of the executive to comply (here it is not), are an insufficient remedy for EU law breaches. *ClientEarth* and *Watson* in the Divisional Court shows that the Court does not take compliance on trust.

42. The Defendants have suggested that the Divisional Court's decision in *Watson* is distinguishable because when that court made its orders: (i) the government had not accepted that amendments were needed; (ii) none were proposed.[29] The submission is therefore that disapplication turns on the government's own view of legality or whether it has made proposals for amendment. This suggests that:

(1) where the government accepts it is acting unlawfully, the Court should be less inclined to order disapplication; and

(2) merely by advancing a proposal for consultation, the government may avoid disapplication of legislation which it concedes is incompatible with directly effective EU law.

43. Such a result would fail to give full effect to EU law. The government's acceptance of illegality, but continued application of an unlawful regime, strengthens the case for disapplication.

(3) Length of suspension of order for disapplication

44. The Defendants, on 28 July 2017, stated in correspondence, in response to Liberty's proposed order for disapplication from 1 January 2018:[30]

> "Even if the suspended order [for disapplication] you propose were appropriate, it could not in practice take effect before 31 July 2018 and would have to be subject to a liberty to apply provision, bearing in mind the range of possible outcomes following consultation, possible delays in Parliament's ability to consider amendments, and time needed for them to take effect."

[29] GLD/BM (28 July 2017) ¶12.

[30] GLD/BM (28 July 2017) ¶13.

45. Liberty agrees that a suspended order for disapplication from 31 July 2018 is appropriate.

46. Such an order is, if anything, generous in circumstances where:

    (1) Liberty wrote to the Defendants in February 2017 explaining that Part 4 was incompatible with EU law, including on the grounds now conceded or undefended.[31]

    (2) The Defendants refused to respond substantively to pre-action correspondence.

    (3) The Defendants, having taken the position in their 6 April 2017 SGR that the entire claim was unarguable, reversed this on 7 July 2017 and concede the incompatibilities mentioned above.

    (4) Part 4 commenced on 30 December 2016, without the key safeguard of judicial prior authorisation of retention notices. Part 4 has therefore been in force for over 13 months, and over 7 months since the Defendants conceded its incompatibility. Unlawful retention of and access to communications data has continued for the entire period for which Part 4 has been in force.

    (5) The government's consultation on proposed amendments closed on 18 January 2018. So far as Liberty is aware, no response has been announced, and there is no proposed timetable for preparation of amendments in light of consultation responses or for parliamentary debate.

47. There has been ample time to correct the conceded and undefended illegalities.

48. Liberty has no objection to a provision being included in an order for disapplication for liberty to apply (as the Defendants' 28 July letter proposed). But very good reasons for any extension would have to be shown.

---

[31] BM/GLD (21 February 2017); GLD/BM (23 February 2017).

F THE COURT SHOULD DECLARE THAT PART 4 AND THE DEFENDANTS' APPROACH TO MATERIALS COVERED BY LEGAL PROFESSIONAL PRIVILEGE IS UNLAWFUL

49. Part 4 is incompatible with EU law insofar as it does not provide adequate protection for legally privileged communications data. The DGR fail to meet this point and positively assert that legal privilege cannot attach to communications data. This is wrong in law. That this assertion is made in the DGR indicates that the Defendants are, under Part 4, applying a legally flawed approach. The Court should declare this to be the case. The Court should in any event also refer the question of whether *Watson CJEU* or EU law requires certain minimum protections of legal privilege in relation to communications data.

50. **SFG ¶¶69–71, 105–106, 178 and 188** plead that Part 4 is incompatible with EU law insofar as it does not provide specific protection for legal professional privilege. It is well established that ECHR Articles 8 and 10 require special treatment of legally privileged material (see **SFG ¶71**). Further, by CFR Article 52(3), the protection under CFR Articles 7 and 11 is no less than those accorded under ECHR Articles 8 and 10.

51. **DGR ¶135** states (emphasis in original):

> "While communications data might reveal the <u>fact</u> that a person has spoken to their lawyer, or the duration of the conversation, it would not reveal any of the content of the conversation, and therefore would not attract legal professional privilege."

52. The factual statement is correct: communications data may reveal the fact that a person has spoken with their lawyer (or, in addition, that the lawyer has spoken with a third party). But the conclusion that no privileged material would thereby be revealed is: (i) wrong in law; and (ii) contrary to the government's own previous (correct) legal analysis and concessions it had made before the IPT.

53. It is trite law that:

    (1) The description of a party's legally privileged documents is normally itself protected from disclosure, and it is sufficient simply to state that they are "*confidential communications passing between the client and his legal advisers for the purposes of obtaining legal advice*" (or otherwise to state the facts that

ground the privilege, rather than identifying the documents themselves): *Derby v Weldon (No 7)*[32] and *Gardner v Irvin*.[33]

(2) A client's identity or location may be a matter that is subject to legal privilege, where it is communicated to a lawyer in confidence for the purpose of obtaining legal advice: *JSC BTA Bank v Solodchenko (No 3)*[34] and *SRJ v Persons Unknown*.[35] Communications data that reveals the identity and location of a lawyer's client who sends or makes an electronic communication to the lawyer would reveal precisely that information.

(3) The fact of the making of communications that are protected by litigation privilege is itself subject to that privilege.[36]

54. As to the government's own prior (correct) analysis, **Passmore 1 ¶¶27–28** notes:

> "I am also aware of the recent ruling in *Greennet/Privacy International v SSFCA and GCHQ* [2016] UKIP TRib 14_85-CH and 120-126-CH where the contrary proposition to that set out in paragraph 135 of the Grounds of Resistance was conceded by the Government and where amendments were made to GCHQ's internal procedures as a result. (The Tribunal said at [87]: '*the third problem was of metadata, which could attract LPP by reference to communications with lawyers, even without their content. There was no dispute between Counsel that metadata might attract LPP...*'.)
>
> … communications data are a type of metadata. GCHQ's procedures now accept that
>
> 'The concept of LPP applies to: ... Exceptionally, some communications data (i.e. "events" or the fact of a communication)' (see Appendix III to the *Greennet/Privacy International Judgment*, which cites the new procedures in full)."

55. **DGR ¶135** contends that Liberty's SFG did not provide examples of where communications data would be covered by legal privilege. But **Passmore 1 ¶29** gives examples:

---

32 [1990] 1 WLR 1156, 1179–1180 (Vinelott J). There are exceptions: see, eg, *Stockman v Arricano* [2017] EWHC 1337 (Comm).

33 (1878) 4 Ex D 49, 52–53 (Cotton LJ).

34 [2011] EWHC 2163 (Ch), [2013] Ch 1 [28], [38]–[39] (Henderson J).

35 [2014] EWHC 2293 (QB) [15], [21], [27] (Sir David Eady).

36 See generally Hollander, *Documentary Evidence* (12th ed, 2015) [18-01].

29.1 The fact that the client has consulted a lawyer (or a particular lawyer with a particular specialism at a particular firm) may itself be subject to legal advice privilege. In some circumstances, my clients would be entitled to claim privilege over the fact that they have taken legal advice, as well as over its content. Further, a client is entitled to assert privilege as to who they have taken legal advice from. Communications data alone will reveal (or suggest) the fact that such advice has been taken. This may be sensitive information given that certain legal advisers and firms, particularly in relation to the criminal law, are known for their expertise in a very focused and limited area.

29.2 The fact that a lawyer for the purposes of litigation has approached a potential witness, as well as the identity of the witness, are subject to litigation privilege. For example, in litigation I might manage to trace and take a draft witness statement from a relevant witness. The fact that I have traced and approached the witness is itself privileged. It need not be disclosed. The communications data alone will reveal (or suggest) that fact."

56. As mentioned, **Passmore 1 ¶¶13–25** also explains the chilling effect that Mr Passmore, an experienced practitioner including in white collar crime, has increasingly noticed in clients communicating with him as their lawyer. And as noted above, his evidence is unchallenged.

57. The Defendants are therefore proceeding on the legally incorrect basis that communications data cannot be subject to legal professional privilege. The Court should make a declaration as to the correct position and refer to the CJEU the question of what, if any, mandatory minimum safeguards should apply to privileged material.

G THE COURT SHOULD REFER QUESTIONS ON THE *WATSON* REQUIREMENTS IN THE CONTEXT OF PART 4 TO THE CJEU

58. The parties accept that the scope and extent of some of the mandatory safeguards identified by the CJEU in *Watson* are not *acte clair*. The Court is therefore invited, under TFEU Article 267, to refer questions to the CJEU. Indeed, *Watson CA* effectively binds this Court to hold that certain *Watson* requirements on which Liberty relies are uncertain as a matter of EU law.

59. The Court is invited to request that the CJEU expedite the reference, given the importance of the issues. Any reference should probably be heard with the reference

already made by the Investigatory Powers Tribunal (the "**IPT**") in Case No IPT/151/110/CH (the "**IPT Reference**"), on related but distinct questions.

60. The Defendants had not, prior to the DGR, provided any substantive response to the SFG and in particular the pleaded *Watson* requirements. Liberty therefore sets out a detailed response to the arguments in the DGR in the Annex to this skeleton argument. It is not, however, intended that the Court resolves the parties' competing positions now. Liberty instead identifies those issues that ought to form the basis of a reference.

(1) Several important *Watson* requirements are now uncertain in light of *Watson CA*

61. Lord Lloyd-Jones (giving the judgment of the Court of Appeal) held in *Watson CA* that:

(1) **Application of EU law to retention for the purpose of protecting national security:** The Court should not rule on whether the requirements in *Watson CJEU* applied where the purpose of retention/access is national security, "*to avoid pre-empting matters which will have to be considered on the reference by the IPT*".[37]

(2) **Retention in the EU:** There was "*considerably uncertainty*" about whether the CJEU's unqualified statement that "*national legislation must make provision for the data to be retained within the European Union*"[38] was subject to qualification, and the Court of Appeal should not "*make a definitive statement … in the form of a declaration*".[39]

(3) **Notification of access to retained data:** The Court should not give declaratory relief in relation to the requirement that "*the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities*".[40] The point had only briefly been raised in the national proceedings (and was not mentioned in the order for reference), was not included in the

[37] *Watson CA* [12].

[38] *Watson CJEU* [122].

[39] *Watson CA* [19].

[40] *Watson CJEU* [121].

CJEU's *dispositif* (the significance of which was "*not entirely clear*"), and the IPT's reference would address this.[41]

(4) **Limitation of data retained:** Lord Lloyd-Jones was initially minded to accept that provisions permitting retention must "*proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious criminal offences*".[42] However, without rejecting the argument, he ultimately accepted that this requirement in *Watson CJEU* was "*not necessarily susceptible of automatic application*" to DRIPA.[43] He also held that declaratory relief was inappropriate because the point was not raised in *Watson* and is a live issue in the present claim.[44]

62. The Court of Appeal reached these conclusions having considered, and rejected, the Defendant's arguments that those requirements did not exist (or were otherwise than the claimant–respondents had submitted).[45]

63. Each of these points, and some further issues, should be the subject of a reference to the CJEU. Those questions are:

(1) Three threshold issues for the extent of application of EU law:

(a) **Application of *Watson CJEU* to purpose of protecting national security:** Liberty contends (**SFG ¶¶80–82, 172**), and the Defendants deny (**DGR ¶95**) that the *Watson* requirements apply to retention/access for the "*national security purposes*" (those in ss 61(7)(a) and (c)) and "*in relation to the activities of the Security and Intelligence Agencies*". As mentioned, the Court of Appeal considered it inappropriate to decide this issue in view of the IPT's reference.

---

41 *Watson CA* [21].

42 See *Watson CA* [23]–[24] (Lloyd-Jones LJ).

43 See *Watson CA* [26(2)] (Lloyd-Jones LJ).

44 See *Watson CA* [26(1)], [26(3)] (Lloyd-Jones LJ).

45 See *Watson CA* [11] (First Defendant's argument that the reasoning in *Watson CJEU* is limited to the purpose of preventing or detecting crime and does not extend to national security), [17] (First Defendant's submission of "*deep uncertainty*" about the requirement to retain data within the EU), [25]–[26] (Fist Defendant exceptionally made submissions after draft judgment on whether retention must be limited to a defined public whose data was likely to reveal a direct or indirect link with serious criminal offences).

(b) **Application of *Watson CJEU* to entity data:** The Defendants contend for the first time in **DGR ¶96** that *Watson CJEU* does not apply to "*entity data*" as defined in s 261. For the reasons in paragraph 73(2) in the Annex, Liberty considers this to be incorrect.

(c) **Relevance of non-binding codes of practice under EU law: SFG ¶¶61 and 88–89** explain that the mandatory minimum safeguards under *Watson CEJU* must be contained in an instrument that has the force of law and, therefore, may not be contained merely in codes of practice. Accordingly, codes of practice cannot be considered when determining whether those mandatory minimum safeguards on the power to retain and access communications data exist and are sufficient. It is unclear whether the Defendants contest this, but **DGR ¶130** (for example, which relies on provisions of a code of practice) suggest it does.

(2) **Whether a general and indiscriminate retention regime exists:** Part 4 permits general and indiscriminate retention of communications data because the data retained is not limited by reference to categories of data, means of communication or persons concerned[46] and/or Part 4 "*does not proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious criminal offences*".[47] The Court of Appeal was initially minded to accept this requirement but, ultimately, considered it uncertain.

(3) Other *Watson* requirements:

(a) **Retention and access not limited to <u>serious</u> threats to s 61(7) interests: SFG ¶171(1)** explains that Part 4 enables general and indiscriminate retention of communications data because it is not based on serious threats to the interests in s 61(7), and therefore allows the issue of a warrant for purposes that are not capable of justifying an interference with Article 7 and

---

46 *Watson CJEU* [106], [108], [110]–[111],

47 See *Watson CA* [23], [25(3)] (Lloyd-Jones LJ).

8 rights.[48] **DGR ¶111(c)** contests this, for reasons Liberty explains in paragraphs 74–75 in the Annex below to be incorrect.

(b) **No notification of access to retained data:** The failure to notify the target whose data is accessed, once it is operationally safe to do so, makes Part 4 incompatible with EU law. Existing notification procedures are insufficient to satisfy this requirement. In addition there is no provision for notification of retention of data.

(c) **No requirement to retain in the EU: SFG ¶174(5)** pleads that communications data must be retained within the EU.[49] **DGR ¶128–129** contest this. *Watson CA* considered this uncertain.

(4) **Legally privileged materials:** The Court should, in addition to granting the declaratory relief sought in Part F above, refer the issue of whether Part 4 is incompatible with EU law insofar as it does not provide adequate protection for legally privileged communications data and, in particular, whether this too is a mandatory minimum requirement.

(2) A reference is the appropriate vehicle to resolve these issues

64. Liberty has, since August 2017, suggested that a reference would be required in order to determine at the least the national security issue (in paragraph 74(1) below). Liberty submits that it would be sensible to refer <u>all</u> issues and *Watson* requirements above to the CJEU, in view of:

(1) the Court of Appeal's conclusions and approach in *Watson CA*;

(2) the IPT Reference, which Liberty understands to remain pending at the early stages (and to which this reference could usefully be joined);

---

48 This is true also of Article 11 rights.

49 *Watson CJEU* [122]: "*In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 66 to 68).*"

(3) the apparent need to resolve all of the issues above, promptly and in the context of Part 4; and

(4) the interconnected nature of the issues and requirements set out above, which makes consideration of them together desirable.

65. The Defendants have suggested at various points that no reference should be made in this case, for two reasons. Neither withstands scrutiny:

(1) The Defendants have argued that the lawfulness of Part 4 "*is likely to be further clarified in the context of pre-existing litigation before the Investigatory Powers Tribunal*" in the IPT Reference, in particular the national security question.[50] This is a bad point:

(a) The Defendants accept that the CJEU's ruling on the IPT Reference may only be relevant to, not determinative of, the application of EU law to retention/access under Part 4 for national security purposes.[51]

(b) The IPT has referred questions that concern whether "*a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies*" falls within the scope of EU law and the e-Privacy Directive.[52] The reference is concerned with (i) a different, general and sparse regime (s 94 of the Telecommunications Act 1984),[53] (ii) under which communications data could be required to be delivered up to SIAs but which does not permit a direction to a telecommunications operator to retain data (a critical difference to DRIPA,

---

50 Defendants' Submissions on Claimant's Application for a Costs Capping Order (29 August 2017) ¶25.

51 **DGR ¶95** states: "*The CJEU's ruling on the reference from the IPT will determine (or at least be highly relevant to) the question of whether EU law applies to eh use of Part 4 for the purposes of national security …*"

52 Order for Reference of the IPT in Case No IPT/15/110/CH (18 October 2017) (see **DGR ¶57**, which set this out).

53 Section 94(2) provides: "*If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom the section applies, give to that person a direction requiring him (according to the circumstances of the case) to do or not to do, a particular thing specified in the direction.*" Section 94(2) applies to OFCOM and "*providers of public electronic communications networks*": s 94(8).

and thus to Part 4, which the IPT itself pointed out),[54] and (iii) which applies only in relation to national security (or foreign relations). The IPT's Reference cannot resolve such issues as:

(i) whether *Watson CJEU* applies to "entity data" (this not being a term used in the Telecommunications Act 1984) — see paragraph 74(2) in the Annex below;

(ii) whether retention of and access to communications data in Part 4 is general and indiscriminate;

(iii) how a communications data retention/access regime must:

(A) provide for notification of affected persons— see paragraph 77(2) in the Annex below;

(B) require communications data retained by telecommunications operators to be retained in the EU (as distinct from communications data provided by them to the SIAs under the Telecommunications Act) — see paragraph 77(3) in the Annex below;

(iv) whether and how a communications data retention/access regime must provide special protection for legally privileged materials (including legally privileged materials) — see paragraphs 49-57 above.

(c) Further, the IPT Reference may not resolve the question of application in relation to national security in a way that applies to Part 4. If the CJEU answers the first question referred to the effect that EU law and/or the e-Privacy Directive do not apply to the exercise of s 94 powers, the CJEU will not need to, and almost certainly will not,[55] consider the content of the

[54] IPT Reference Decision [19].

[55] The CJEU frequently declines to answer questions it considers unnecessary to dispose of the national proceedings, as occurred in *Watson CJEU* [126]–[133].

Watson requirements. This would leave EU law as to the content and application of the *Watson* requirements here no clearer.

(2) **Possibility of amendment is no reason not to refer:** The Defendants have also suggested (cf **SGR ¶46**) that by the time the CJEU decides any reference, Part 4 will have been amended. As to this, there is current and ongoing illegality and the Claimant is entitled to seek a ruling as to the lawfulness of the regime in dispute under which this unlawful action occurs.

66. The Defendants have now resiled from the position that no reference should be made. They now say that a reference should be made if the Court is minded to rule against them on any of the issues above: **DGR ¶108**. But in light of *Watson CA* it is plain that the issues are not clear in either direction. Further, there is little to be gained by referring some but not all of the issues and questions identified above.

H THE CLAIM AGAINST PART 4 IS NEITHER PREMATURE NOR FUTILE

67. The Defendants seek, again,[56] to re-litigate their arguments of prematurity and futility that Jeremy Baker J rejected when granting permission.[57]

68. **SGR ¶46** said:

> "The Government has accepted that Parts 3 and 4 of the Act require close scrutiny and potential amendment in the light of the CJEU's judgment in *Watson*. The Government is presently considering the need to bring forward legislative proposals to amend Parts 3 and 4 (as well as reviewing the associated statutory codes) in order to comply with the CJEU's judgment. A judicial review challenge to a legislative regime which has already been conceded to require careful scrutiny, and potential amendment, in order to ensure compliance with EU law, is likely to be futile and, like the other parts of the claim, should properly wait until the legislative regime, with any necessary amendments, is in a settled state."

69. Jeremy Baker J rejected the argument when giving permission:

---

[56] Defendants' Submissions on Claimant's Application for a Costs Capping Order (29 August 2017) ¶25.

[57] Permission Order p 2 (Observations).

"Although the Defendants state that the Government is presently considering the need to bring forward legislative proposals to amend Parts 3 and 4 of the IPA, as well as reviewing associated statutory codes, in order to comply with the CJEU's judgment in Watson, as Part 4 is presently in force, the Claimant is entitled to pursue that part of its application at this stage."

70. Part 4 remains in force. **DGR ¶82** states in terms that Part 4 "*is already substantially in force*". It remains the case, more than 14 months after commencement, that no code of practice for retention of communications data has been made under Schedule 7 (**DGR ¶106**).[58]

71. Further, for the same reasons as those in paragraphs 39–43, neither the Defendants' concessions, nor proposals or consultation, make any difference to this. And in any case no guarantee of any change can be given: Parliament has the last word (as **DGR ¶85(c)** accepts).

I CONCLUSION AND ORDERS

72. For the reasons above, the Court should:

(1) Disapply the provisions set out in paragraph 24 above, that order being suspended to 31 July 2018, and declare that they and have at all times since they entered into force been unlawful;

(2) Declare that Part 4 is unlawful insofar as it fails to make any provision for protection of legally privilege material and that the Defendants' are acting unlawfully in applying Part 4:

(a) on the incorrect basis in law that communications data cannot attract legal professional privilege;

(b) without specific provisions to protect communications data subject to legal professional privilege; and

[58] The Defendants instead say they apply two different codes of practice: GLD/BM (29 August 2017) ¶9.

(3) Refer the issues identified in paragraph 63 above to the CJEU, in order to obtain a directly applicable ruling on the mandatory minimum requirements of EU law in the context of Part 4.

73. Costs should be dealt with upon the Court giving judgment.

MARTIN CHAMBERLAIN QC
Brick Court Chambers

BEN JAFFEY QC
Blackstone Chambers

DAVID HEATON
Brick Court Chambers

8 February 2018

BHATT MURPHY

ANNEX: LIBERTY'S SUBSTANTIVE SUBMISSIONS ON THE ISSUES OF EU LAW

74. **First**, in relation to the extent of application of the *Watson* requirements and the basis on which they may be satisfied, the issues are as follows:

(1) **Application of *Watson CJEU* to purpose of protecting national security:** Liberty contends (**SFG ¶¶80–82, 172**), and the Defendants contest (**DGR ¶95**) that the *Watson* requirements apply to retention/access for the "*national security purposes*" (those in ss 61(7)(a) and (c)) and "*in relation to the activities of the Security and Intelligence Agencies*". As mentioned, the Court of Appeal considered it inappropriate to decide this issue in view of the IPT's reference.

(2) **Application of *Watson CJEU* to entity data:** The Defendants contend for the first time in **DGR ¶96** that *Watson CJEU* does not apply to "*entity data*" as defined in s 261. This argument is wrong:

(a) **DGR ¶97** misquotes the definition of "*location data*", omitting a material part. Those definitions in Article 2[59] (with the text omitted or incorrectly set out in the DGR underlined) are:

> "(b) '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;
>
> (c) 'location data' means any data processed <u>in</u> an electronic communications network <u>or by an electronic communications service</u>, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service; …"

(b) Section 261(3) defines entity data as follows:

> "'Entity data' means 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,

[59] As amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337/22, although the amendments did not affect the definition of "location data".

(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."

"*Entity*" is defined in s 261(7) as "*a person or thing*". "*Events data*" is defined in s 261(7) 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."

(c) The definitions in the e-Privacy Directive and the IPA do not map neatly onto one another. In consequence, it is not difficult to identify examples of where "*entity data*" as defined in s 261 is "traffic data" or "location data", so that the premise for the asserted non-application of the *Watson* requirements is wrong:

(i) The address and specific location of a fixed line terminal (such as a landline telephone, fax or fibre cable connection point, say in a home or office) are "*location data*". A billing address and billing (eg bank account or credit card) details fall within the definition of "*traffic data*" — they will be used for billing for the conveyance of electronic data. (They are also "*communications data*" under s 261(5) as they are or are capable of being held or obtained by or on behalf of a telecommunications operator, are about the entity to which a telecommunications service is provided, and relate to the provision of the service.)

(ii) But these are all "*entity data*" under the IPA: they do not describe an event consisting of engaging in specific activity at a specific time (so are not "*events data*"), they are data about a person/thing and/or its association with (part of) a telecommunications service, and they are/include data that identifies/describes the entity, including its location.

(3) **Relevance of non-binding codes of practice under EU law: SFG ¶¶61 and 88–89** explain that the mandatory minimum safeguards under *Watson CEJU* must be contained in an instrument that has the force of law and, therefore, may not be contained merely in codes of practice. Accordingly, codes of practice cannot be considered when determining whether those mandatory minimum safeguards on the power to retain and access communications data exist and are sufficient. The DGR fail to address this directly, so it remains unclear whether the Defendants contest this. Various references to codes suggest that they might — see, for example, **DGR ¶130** (relying on provisions of a code of practice). *Watson CJEU* accepts that the minimum mandatory requirements must be "*legally binding under domestic law*".[60] In so holding, the CJEU accepted the Advocate General's conclusions that Article 15(1) permits only measures that are "*binding on the national authorities upon which the power to access the retained data is conferred*", that is, "*legislative or regulatory measures*", and not "*codes of practice or internal guidelines having no binding effect*".[61] This flows from the requirement in Article 15(1) of the e-Privacy Directive that derogations must be "*legislative measures*".

75. **Secondly,** Liberty submits that there is general and indiscriminate retention of and access to communications data in breach of the requirements of *Watson CJEU*, due to a **failure adequately to limit the data that may be retained**.

76. **SFG ¶¶96, 100, 101 and 171(2)** explain that Part 4 permits indiscriminate retention of communications data because the data retained is not limited by reference to categories of data, means of communication or persons concerned.[62] As *Watson CA* held, Liberty's claim encompasses the requirement that the retention power in Part 4 "*does not proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious*

---

60 *Watson CJEU* [117].

61 Opinion of Advocate-General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson ECLI:EU:C:2016:572 [150]–[151].

62 *Watson CJEU* [106], [108], [110]–[111],

criminal offences".[63] **DGR ¶112** contests this. But none of the reasons advanced answer Liberty's case:

(1) **DGR ¶112(a)–(e)** point out various provisions of Part 4 that: require the Secretary of state to consider whether a notice is "*necessary and proportionate*"; permit a notice to require retention of less than all communications data by all operators; set a maximum length for retention under the notice; and require the Secretary of State to consider the benefits of the notice and numbers of users affected and to consult with a telecommunications operator. **DGR ¶112(f)** refers to provision for oversight by the Investigatory Powers Commissioner and the Information Commissioner, telecommunications operators to seek review of retention notices, and the Secretary of State to keep notices under review.

All this provides no answer to Liberty's point. Requirements to consider, the possibility of retention of something less all communications data by all telecommunications operators, a maximum retention length and oversight provisions do not impose limits on retention by reference to categories of data, means of communication or persons concerned. Nor do they require the Secretary of State to proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious criminal offences or serious threats to s 61(7) interests. Those provisions accordingly do not show that Part 4 complies with this requirement. They show instead that Part 4 permits generalised and indiscriminate retention.

(2) The suggestions in **DGR ¶113** and **Scurry 1 ¶65** that retention notices have in practice been issued only to 25 telecommunications operators, do not all cover the maximum 12-month period permitted, and do not cover all services provided by or data held/obtainable by (all) the affected operators, and have been revoked or varied, even if correct, is irrelevant. It does not establish that requirements exist to limit retention notices to the extent required by EU law.

> "Mr Eadie accepted that the consequence of this policy stance is that we should test the validity of DRIPA on the assumption that the retention notices issued under it

[63] See *Watson CA* [23], [25(3)] (Lloyd-Jones LJ).

> may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months. The case was argued on both sides on that basis."

The Divisional Court plainly thought this approach was correct. It is. The Defendants now say that this approach was agreed in *Watson* but Mr Scurry has now provided "*a number of details about the number and scope of retention notices that are actually in force*". Assuming the 25 telecommunications operators on whom retention notices are said to have been served (**Scurry 1 ¶65**) are or include the major UK telecommunications operators, it remains entirely possible that retention of virtually all UK communications data may occur (**Stoughton 1 ¶¶34–36**).[64]

77. **Thirdly**, as to the specific mandatory minimum safeguards required by *Watson CJEU*:

(1) **Retention and access not limited to <u>serious</u> threats to s 61(7) interests: SFG ¶171(1)** explains that Part 4 is incompatible with EU law because it is not based on serious threats to the interests in s 61(7), and therefore allows the issue of a warrant for purposes that are not capable of justifying an interference with Article 7 and 8 rights.[65] DGR ¶111(c) says this is "*wholly unparticularised*", but it is a proposition of law, not fact. The argument is one of (obvious) analogy with the CJEU's reasoning in relation to the prevention and detection of serious crime, as follows:[66]

> "Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 60)."

---

64 Notwithstanding that Mr Biggar says the government's approach is to monitor requirements and revoke those that do not add value: see **Biggar 1 ¶22**.

65 This is true also for Article 11 rights.

66 *Watson CJEU* [102].[67] The formalistic point in **DGR ¶122** that the challenge to Part 3 is stayed should be rejected. **SFG ¶174(4)** makes clear that this part of the Part 4 challenge requires consideration both of retention and access (and Liberty has permission to pursue "*the claim <u>in relation to</u> Part 4*": Permission Order ¶1). In any case, access under the current RIPA regime does not provide for post-notification, so ongoing retention of and access to communications data thereunder is on any view unlawful. This is no doubt why **DGR ¶¶123–127** respond at length to the argument.

If only preventing and detecting serious crime is even capable of justifying retention of communications data, so too are only serious threats to the other s 61(7) interests capable of justifying retention. The purposes are: "*public safety*" (s 61(7)(d)); "*preventing death or injury*" (s 61(7)(g)); assisting "*investigations into alleged miscarriages of justice*"; assisting in the identification of a person who is dead or unable to identify themselves (s 61(7)(i)); national security (s 61(7)(a)); threats to economic wellbeing insofar as relevant to national security (s 61(7)(c)). In particular:

(a) There is no difference in principle between the interests these purposes protect and those protected by action for the purpose of preventing/detecting serious crime, such that a less serious threat to the interest should justify retention for purposes other than preventing and detecting serious crime; and

(b) Action for the purpose of preventing and detecting serious crime will often by its nature fall within other s 67 purposes, such as national security, public safety, preventing death or injury, or threats to economic wellbeing relevant to national security. It would be anomalous that a less serious threat to s 61(7) interests cannot justify retention/access for preventing/detecting crime but can justify retention/access for other purposes.

DGR ¶111(c) is therefore wrong to say this has no basis in *Watson CJEU*. It follows from it. The assertion that all s 61(7) purposes (that are not undefended in this claim) are of their nature sufficient to justify interference is not explained, and cannot stand with the CJEU's requirement in relation to preventing/detecting crime.

(2) **No notification after access:** Neither Part 4 nor Part 3 requires notification of any person affected (that is, whose data has been retained or accessed) as soon as

that notification is no longer liable to jeopardise investigations being undertaken.[67] *Watson CJEU* said:[68]

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

The Defendants in response set out various provisions of the IPA, but they do not, individually or collectively, satisfy this requirement:

(a) **DGR ¶124** refers to review by the IPT and assert that an application can be made "*without evidence of wrongdoing*", citing *Kennedy v United Kingdom*. As to this:

(i) This is not a requirement to notify those whose communications data is retained/accessed.

(ii) In any case, **DGR ¶124** says, a person "*who has <u>some basis to believe</u> the investigatory powers have been unlawfully used against them*" may complain to the IPT. This reflects recent IPT jurisprudence, which <u>raised</u> the threshold for an application. Previously it was thought that anyone could apply for investigation of retention of or access to their communications data. The IPT in *Human Rights Watch*

---

[67] The formalistic point in **DGR ¶122** that the challenge to Part 3 is stayed should be rejected. **SFG ¶174(4)** makes clear that this part of the Part 4 challenge requires consideration both of retention and access (and Liberty has permission to pursue "*the claim <u>in relation to</u> Part 4*": Permission Order ¶1). In any case, access under the current RIPA regime does not provide for post-notification, so ongoing retention of and access to communications data thereunder is on any view unlawful. This is no doubt why **DGR ¶¶123–127** respond at length to the argument.

[68] *Watson CJEU* [121].

v Secretary of State for the Foreign and Commonwealth Office,[69] however, departed from this understanding. It held that an applicant had to have an evidential basis that supports something more than an "*asserted general belief*" or a "*potential risk*" that their communications have been monitored (see **SFG ¶20(4)**). The Defendants' quotation from *Kennedy v United Kingdom*[70] — which referred to the position as previously understood — is incorrect.

(b) Liberty accepts that notification is required only when it is no longer necessary to maintain secrecy. The suggested difficulties in **DGR ¶125** therefore do not arise:

(i) It would remain necessary not to notify a person of access if doing so would jeopardise the purpose for which access originally occurred (for example, where an investigation is ongoing) or where this would jeopardise the purpose for which other communications data had been retained or obtained (for example, where there are multiple investigations into the same person).

(ii) Further, and in any event, the feared adverse consequences are exaggerated: communications data is routinely disclosed in criminal prosecutions, but the Defendants have not adduced any empirical (or even anecdotal) evidence to suggest retention and access are less useful because communications data are a staple of almost most criminal prosecutions of serious offences.

(c) **DGR ¶¶126–127** refer to the serious error disclosure regime and assert that this is sufficient to enable persons affected to exercise their right to a legal remedy. This is wrong. The **DGR** fail to address the point in **SFG¶¶174(4) and 115** that Part 8 (ss 229, 233 and 235) require that the Investigatory Powers Commission may notify a person:

---

69 *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15-165-CH [45]–[47].

70 *Kennedy v United Kingdom* (ECtHR, Application No 26839/05, 18 May 2010, Fourth Section) [167].

(i) only where the error is a "*serious error*", that is, where the error has caused the person "*serious prejudice or harm*" — a breach of the ECHR is expressly not of itself sufficient for that purpose (s 231(2)–(3)); and

(ii) only if notification is "*in the public interest*" (s 231(1), (4)).

This is obviously not routine notification to the extent that *Watson CJEU* requires.

(3) **No requirement to retain in the EU: SFG ¶174(5)** pleads that communications data must be retained within the EU.[71] **DGR ¶128–129** contest this, for the same reasons as the First Defendant advanced in *Watson CA*.[72] The Court of Appeal held that this requirement is uncertain as a matter of EU law: see paragraph 62(2) above. This matter can only realistically be resolved by a reference, as **DGR ¶129** recognises.

78. **Fourthly**, and finally, **SFG ¶¶69–71, 105–106, 178 and 188** plead that Part 4 is incompatible with EU law insofar as it does not provide specific protection for legal professional privilege, as mentioned in paragraphs 49 to 57 above. If the Court were not minded to decide that point now, it should refer it in addition to the CJEU.

---

71 *Watson CJEU* [122]: "*In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 66 to 68).*"

72 *Watson CA* [17].