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

Claim No. CO/1052/2017

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

SUMMARY GROUNDS OF RESISTANCE

Introduction

1. This claim is premature. The Claimant ("Liberty") challenges seven parts of the Investigatory Powers Act 2016 ("the Act") on the grounds of alleged failure to meet "foreseeability" and "necessity" requirements under Articles 8 and 10 of the ECHR, and alleged non-compliance with principles of EU law concerning the retention of, and access to, personal data.

2. In order to determine that challenge the Court would need to assess the legal regime and safeguards under each relevant part of the Act, including not only the statutory provisions themselves but non-statutory measures such as codes and guidance, in order to consider whether – having regard to the full legal framework – the regime satisfies the requirements of Articles 8 and 10 ECHR and EU law. Currently: (i) six of the seven impugned parts of the Act are not yet in force; (ii) each of those six parts will, once in force, be supported by a system of detailed safeguards which has not yet been designed, let alone implemented, and by statutory Codes which have similarly not yet been made or adopted; and (iii) the single part of the Act under challenge that *is* now at least partly in force (Part 4 of the Act) is one that the Government has already said it is going to reconsider. In submissions to the Court of Appeal in the claim pursued by Liberty (acting on behalf of Tom Watson MP) to the predecessor legislation to Part 4 of the Act, the Government has made clear that it intends to review Part 4 and Part 3 in the light of the judgment of the Court of Justice of the European Union ("CJEU") dated 21 December 2016 in the linked cases *Tele2 Sverige*

AB v Post-och telestryelsen C-203/15 and *R(Watson) v Secretary of State for the Home Department C-698/15* ("*Watson*").

3. It is also to be noted, in this regard, that a number of the issues raised by Liberty are already under consideration by the Investigatory Powers Tribunal ("the IPT") and the ECtHR (and it is at least possible that will be further issues before the CJEU) in the context of challenges to the statutory regimes that the Act is intended to replace. That fact both creates (so far as the ongoing IPT proceedings are concerned) a risk of parallel proceedings/inconsistent decisions on important points of principle; and indicates that it is likely that the position in principle will clarify or at least alter in the period before the relevant parts of the Act and their accompanying framework come into effect.

4. In the circumstances, permission to bring the claim should be refused on grounds of prematurity: the claim cannot proceed until the relevant legal frameworks are in place and/or until proposed legislative amendments to Part 4 have been brought forward.

5. For the avoidance of doubt, the Defendants do not accept that the claim, or any particular part of it, is arguable. In the sole respect of the claim against Part 4 and compliance with *Watson*, the First Defendant has already conceded in the Court of Appeal that the predecessor legislation to Part 4 of the Act was unlawful in certain respects, and that Part 4 of the Act will need to be carefully considered (and potentially amended) accordingly. The Government will need sufficient time to consider and bring forward any legislative changes that are required to comply with EU law.

Context

6. The Act provides an updated framework for the use of investigatory powers to obtain communications and communications data by the United Kingdom's security and intelligence agencies, law enforcement agencies and other public authorities. The powers provided for under the Act include powers relating to the interception of communications, the retention and acquisition of communications data, the use of equipment interference, and the acquisition and use of bulk data. The Act will replace and update powers previously contained in various other enactments, including the Regulation of Investigatory Powers Act 2000 ("RIPA"), the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), the Wireless Telegraphy Act 2006, the Telecommunications Act 1994 and the Intelligence Services Act 1994.

7. The Act received Royal Assent on 29 November 2016. By section 272(1) of the Act, subject to certain immaterial exceptions for specific provisions, the Act "*comes into force on such day as the Secretary of State may by regulations appoint; and different days*

may be appointed for different purposes". The bulk of the Act is not yet in force. In relation to those parts of the Act that are challenged by Liberty[1]:

(1) Part 6 Chapter 1 of the Act ("bulk interception warrants") is not yet in force.

(2) Part 6 Chapter 2 of the Act ("bulk acquisition warrants") is not yet in force.

(3) Part 6 Chapter 3 of the Act ("bulk equipment interference warrants") is not yet in force.

(4) Part 5 of the Act ("equipment interference warrants") is not yet in force.

(5) Part 4 of the Act (concerning the retention of communications data) has been brought into force in part, with effect from 30 December 2016. However, certain provisions of Part 4 are either not yet in force (sections 89, 91 and 96) or are only partially in force (sections 87, 90 and 94).

(6) Part 3 of the Act (concerning the acquisition of communications data) is not yet in force[2].

(7) Part 7 of the Act (warrants for the retention of "bulk personal datasets") is not yet in force.

8. Section 241 of, and Schedule 7 to, the Act make provision for statutory Codes of Practice to be issued in relation to the exercise of powers under the Act. In particular:

(1) By §1(1) of Schedule 7, the Secretary of State must issue one or more Codes of Practice about the exercise of functions conferred by virtue of the Act.

(2) By §2 of Schedule 7, each Code must include provisions designed to safeguard various public interests, such as (by way of example) the confidentiality of journalistic sources, legally privileged information, and MPs' communications.

(3) By §3 of Schedule 7, any Code about the exercise of functions conferred by Part 3 (acquisition of communications data) must contain various detailed provisions relevant to safeguarding communications data held by public authorities by virtue of that Part.

(4) The Secretary of State must prepare and publish a draft of any Code, and consider representations upon it, before it is published, and may modify the draft as a result: see §4(1), Schedule 7. She must consult the Investigatory Powers Commissioner, and in the case of a Code relating to the exercise of functions

[1] See SFG, §18(1)-(6)

[2] Subject to one small exception. Section 61(7) of the Act, which falls within Part 3, is partially in force for the purposes only of the operation of retention powers under Part 4.

conferred by Part 4 (retention of communications data), must also consult the Information Commissioner: see §4(2), Schedule 7.

(5) Codes of Practice come into force in accordance with regulations made by the Secretary of State. Such regulations must be laid before, and approved by, a resolution of each House of Parliament. When such regulations are laid, the Code to which they relate must also be laid before each House: see §§4(3)-(5), Schedule 7.

(6) If the Secretary of State wishes to revise the whole or part of a Code, such revision requires the same consultation with the public, the Investigatory Powers Commissioner and the Information Commissioner, and the same Parliamentary approval, as the initial making of that Code: see §5, Schedule 7.

(7) A person must have regard to a Code of Practice when exercising any functions to which the Code relates. Although a person's breach of a Code does not of itself render that person liable to criminal or civil proceedings, the Code is admissible in evidence in such proceedings. A Court may take any breach of the Code into account in determining any question arising in those proceedings. Further, the Investigatory Powers Commissioner, any other Judicial Commissioner, the Information Commissioner, and the IPT may take into account a failure by a person to have regard to a Code when determining a question which arises in connection with the exercise of functions to which the Code relates. See §6, Schedule 7.

9. The Defendants intend that the various relevant powers provided for by the Act should come into force concurrently with, or after, the promulgation of statutory Codes of Practice governing the exercise of those powers. The Defendants also intend that, at the same time, detailed internal safeguards for the operation of the powers by the various relevant public authorities should come into operation.

10. As matters currently stand, the factual position regarding the powers challenged by the Claimant is as follows.

Part 6, Chapter 1: bulk interception warrants

11. Part 6, Chapter 1 of the Act will not be commenced before early 2018 (at the soonest). A draft Code of Practice governing interception of communications (both in bulk and under targeted warrants) was published in February 2017, and is presently the subject of a public consultation ending on 6 April 2017. The Code of Practice is expected to be laid before Parliament as soon as reasonably practicable after the end of the public consultation, with a view to it coming into force within a few months thereafter. Internal safeguards consequent upon the Code and Act would be put in place subsequently, but *prior to* the commencement of the powers in Part 6, Chapter 1 of the Act.

12. The draft Code of Practice runs to some 122 pages, and contains numerous detailed provisions governing the exercise of bulk interception powers, and the nature of the safeguards required when exercising those powers.

13. Pending the commencement of Part 6, Chapter 1 of the Act, bulk interception will continue to be governed by Part 1, Chapter 1 RIPA. The extant legislative regime is overlaid by the Interception of Communications Code of Practice, which was last updated in January 2016, and which remains in force. The new powers in the Act contain a number of further safeguards not present in the current regime (to give just one example, a requirement that warrants be approved by a Judicial Commissioner: see s.138(1)(g) and s.140 of the Act). Further safeguards will be contained in the new Code of Practice and in internal arrangements consequent upon the Act. It is a mandatory statutory requirement that such arrangements exist: see s.150 of the Act.

14. Liberty has previously challenged the exercise of bulk interception powers under Part 1, Chapter 1 RIPA before the IPT: see *Liberty and ors v GCHQ and ors* [2015] HRLR 2 and [2015] HRLR 7. The IPT held that the existing bulk interception regime is compatible with Articles 8 and 10 ECHR following the Government's public disclosure of certain internal safeguards.

15. Liberty has lodged an application with the European Court of Human Rights ("ECtHR"), challenging the IPT's conclusions and asserting breach of Articles 8 and 10 ECHR on many of the same grounds that are advanced in the current claim. The application, which has been brought jointly with various other human rights organisations raising similar issues, remains pending before the ECtHR (*10 Human Rights Organisations v UK, app. no. 24960/15*). Two further applications raising similar issues are also before the ECtHR (*Big Brother Watch v UK, app. no. 58170/13* and *Bureau of Investigative Journalism and Alice Ross v UK, app. no. 62322/14*).

16. Thus, the ECtHR will be ruling upon a number of issues concerning Articles 8 and 10 ECHR, that are materially identical to issues that have been raised by Liberty in this claim. For example, Liberty's principal assertion in this claim is that the power to issue bulk interception warrants is incompatible with Articles 8 and 10 ECHR because those warrants are not (i) limited by reference to an individual/set of premises, and/or (ii) permitted only where there is some factual basis to suspect an identified individual of wrongdoing (SFG §108). Precisely the same issues will be addressed by the ECtHR, in respect of the equivalent provisions of RIPA, in each of the *10 Human Rights Organisations, Big Brother Watch* and *Bureau of Investigative Journalism* applications (a point recognised at SFG §62).

Part 6, Chapter 2: bulk acquisition of communications data

17. Part 6, Chapter 2 of the Act will not be commenced before early 2018 (at the soonest). A draft Code of Practice governing the bulk acquisition of communications data was published in February 2017, and is subject to public consultation ending on 6 April 2017. The Code of Practice is expected to be laid before Parliament as soon as reasonably practicable after the end of the public consultation, with a view to it coming into force within a few months thereafter. Internal safeguards consequent upon the Code and Act would be put in place subsequently, in time for the commencement of the relevant part of the Act.

18. The draft Code of Practice runs to around 50 pages, and contains numerous detailed provisions governing the exercise of bulk acquisition powers, and the nature of the safeguards required when exercising those powers.

19. Bulk acquisition of communications data is currently provided for under s.94 of the Telecommunications Act 1984. The new powers in the Act contain a number of safeguards not present in the current regime (including, for example, the approval of warrants by Judicial Commissioners: s.158(1)(e) and s.159 of the Act). Further safeguards will be contained in the new Code and arrangements made under the Code.

20. The IPT has ruled upon the compatibility of the current regime for bulk acquisition of communications data with the ECHR: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and ors* [2016] UKIPTrib 15_110-CH. It held on 17 October 2016 that the bulk communications data regime was not sufficiently accessible/foreseeable for the purposes of Article 8 ECHR prior to 4 November 2015, but was so thereafter, following the publication of *"handling arrangements"*: see the judgment at §101. It adjourned issues of proportionality and compatibility with EU law for later determination, and has not yet ruled upon them.

Part 6, Chapter 3: bulk equipment interference warrants

21. Part 6, Chapter 3 of the Act will not be commenced before early 2018 (at the soonest). A draft Code of Practice governing equipment interference (both in relation to targeted equipment interference under Part 5 of the Act and in relation to bulk equipment interference under Part 6, Chapter 3) was published in February 2017, and is subject to public consultation closing on 6 April 2017. The Code of Practice is expected to be laid before Parliament as soon as reasonably practicable after the end of the public consultation, with a view to it coming into force within a few months thereafter. Internal safeguards consequent upon the Code and Act would be put in place subsequently, in time for the commencement of the relevant part of the Act.

22. The draft Code of Practice runs to over 130 pages, and contains numerous detailed provisions governing the exercise of equipment interference powers, and the nature of the safeguards required when exercising those powers.

23. Operations that would in future be carried out under Part 6, Chapter 3 of the Act would currently be possible under the Intelligence Services Act 1994, which is supplemented by a Code of Practice issued in January 2016. The powers in the Act contain a number of further safeguards not present in the current regime (to give just one example, a requirement that warrants be approved by a Judicial Commissioner: s.178(1)(f) and s.179 of the Act). Further safeguards will be contained in the new Code and in arrangements made under the Act (such arrangements being required by s.191 of the Act).

24. As with the bulk interception powers in RIPA, the IPT has ruled upon the compatibility with the ECHR of the regime permitting equipment interference in the Intelligence Services Act 1994. It has held that (since February 2015) the regime has been compatible with Article 8: see *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and ors* [2016] UKIP Trib 14_85-CH. The claimants in that case have since challenged that conclusion: (i) they have applied for judicial review. Their application was rejected on the basis that the court had no jurisdiction (*R(Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin)). The claimants have however appealed to the Court of Appeal. Their appeal remains outstanding. They have also lodged an application to the ECtHR challenging the IPT's conclusions, as is apparent from a Privacy International press release dated 5 August 2016.

Part 5 of the Act: equipment interference

25. Part 5 of the Act will not be commenced before early 2018 in relation to the security and intelligence agencies and the Ministry of Defence, and before April 2018 in relation to law enforcement agencies (at the soonest). As stated above, a draft Code of Practice governing equipment interference was issued in February 2017, and is subject to public consultation closing on 6 April 2017. The Code of Practice is expected to be laid before Parliament as soon as reasonably practicable after the end of the public consultation, with a view to it coming into force within a few months thereafter. Internal safeguards consequent upon the Code and Act would be put in place subsequently, in time for the commencement of the relevant part of the Act.

26. The draft Code of Practice runs to over 130 pages, and contains numerous detailed provisions governing the exercise of equipment interference powers, and the nature of the safeguards required when exercising those powers.

27. The type of equipment interference authorised under Part 5 of the Act is currently governed by the Intelligence Services Act 1994 (in relation to the security and intelligence agencies) and the Police Act 1997 (in relation to law enforcement agencies). As stated above, a Code of Practice in respect of equipment interference was issued in January 2016, governing the security and intelligence agencies' use of

equipment interference powers under the Intelligence Services Act 1994. The new powers in the Act contain a number of further safeguards not present in the current regime (to give just one example, a requirement that warrants be approved by a Judicial Commissioner: ss. 102-108 of the Act). Further safeguards will be contained in the new Code and in arrangements made under the Act (such arrangements being statutorily required by s.129 of the Act).

28. Again, the IPT has ruled upon the compatibility of the regime under the Intelligence Services Act 1994 with the ECHR, and has held that since February 2015 the regime is compatible with Article 8: see *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and ors* [2016] UKIP Trib 14_85-CH, cited above. In particular, the IPT has held that the regime permits the issue of so-called "thematic" warrants[3], and that the issue of such warrants under the regime is in principle consistent with Article 8 ECHR. As set out above, the claimants in that case have applied for judicial review, and lodged an application at the ECtHR, challenging that conclusion.

Part 4 of the Act: retention of communications data

29. The retention of communications data by communications service providers ("CSPs") was until recently governed by section 1 of DRIPA, which was repealed on 30 December 2016. Communications data retention is now governed by Part 4 of the Act, which (unlike the other provisions attacked by Liberty in this claim) is partially in force. However, certain important provisions (such as the requirement in section 87(1)(b) of the Act for a Judicial Commissioner to approve retention notices) have not yet been commenced. Moreover (as set out below) the provisions of Part 3 of the Act, which will govern the ability of public authorities to *access* retained communications data, are not yet in force. Pending the commencement of those provisions, access to (also referred to as "acquisition" of) communications data continues to be governed by Part 1, Chapter 2 of RIPA.

30. Retention notices that were in force immediately prior to DRIPA's repeal remain in force pursuant to transitional arrangements[4] until 30 June 2017, when they must be replaced by new notices under Part 4 of the Act. Those new notices will, in turn, need to be replaced by no later than three months following the commencement of section 87(1)(b) of the Act (see above): see Schedule 9§4 of the Act.

31. The provisions in Part 4 of the Act are currently under review in the light of the ruling of the CJEU in *Watson*, which concerned (*inter alia*) the compatibility of the data retention regime in section 1 of DRIPA with EU law. In submissions to the Court of Appeal dated 1 March 2017 the Home Secretary has: (i) informed the Court

[3] In the present claim, Liberty does not "*at present*" otherwise challenge the powers in Part 5, including those in section 101(1)(a) of the Act concerning "targeted" equipment interference warrants: see SFG §18(4) and fn 12.

[4] See section 270 and Schedule 9 para 3 of the Act.

of Appeal that she no longer pursues the joined appeals which gave rise to the reference to the CJEU: (ii) invited the Court of Appeal to uphold the Divisional Court's declaration that section 1 DRIPA was inconsistent with EU law, albeit with certain clarifications to reflect the findings of the CJEU; and (iii) indicated that detailed consideration is already being given to the provisions of the Act in the light of the CJEU's judgment. The First Defendant will bring forward any such proposals as are necessary to amend the Act to take account of the CJEU's judgment and the outcome in the Court of Appeal.

32. Further, a new Code of Practice in relation to Part 4 of the Act will be, but has not yet been, adopted. A draft Communications Data Code of Practice (covering both the retention of data under Part 4 of the Act and the acquisition of data under Part 3 of the Act) was published in October 2016, during the passage of the Act (and specifically to aid consideration of the Act in the House of Lords). It contains detailed provisions governing the exercise of data retention powers, and the nature of the safeguards required when exercising those powers. Following the judgment in *Watson* and the potential need for amendments to Parts 3 and 4 of the Act in the light of that judgment, the draft Code of Practice may well require revision before being put out for public consultation. Public consultation and subsequent Parliamentary approval of the Code will take place once any necessary revisions have been made to Parts 3 and 4, and to the Code.

Part 3 of the Act: acquisition of communications data

33. The acquisition of communications data retained by CSPs continues to be governed by Part 1, Chapter 2 of RIPA. The timescale for bringing Part 3 of the Act into force is currently under review given that, as in the case of the retention notice regime under Part 4 of the Act, the Government is presently considering whether and to what extent Part 3 of the Act will require amending to ensure that it complies with the judgment of the CJEU in *Watson* (which concerned both the retention provisions under DRIPA and the acquisition provisions under RIPA). The Government expects that the commencement of Part 3 of the Act will be deferred until any necessary amendments are made.

34. As set out above, a draft Code of Practice, concerning both acquisition and retention powers, was published during the passage of the Act but has not yet been put out for public consultation, given the need to consider the extent to which any changes to Parts 3 and 4 of the Act are required in light of *Watson*. In the meantime, the existing Code of Practice for the acquisition and disclosure of communications data (last updated in March 2015) remains in force.

Part 7 of the Act: bulk personal dataset warrants

35. Part 7 of the Act, governing the holding of and access to bulk personal data, is not expected to be commenced before March 2018 (at the earliest). A draft Code of Practice was issued in February 2017, and is subject to public consultation closing on 6 April 2017. The Code of Practice is expected to be laid before Parliament as soon as reasonably practicable after the end of the public consultation, with a view to it coming into force within a few months thereafter. Internal safeguards consequent upon the Code and Act would be put in place subsequently, in time for the commencement of the relevant part of the Act. Such safeguards are required by statute (see s.221 of the Act).

36. The draft Code of Practice runs to 70 pages, and contains numerous detailed provisions governing the holding of and access to bulk personal datasets, and the nature of the safeguards required when exercising those powers.

37. The type of activity authorised under Part 7 is currently authorised by the Security Service Act 1989 and the Intelligence Services Act 1994, read with published handling arrangements for the holding of and access to bulk personal data. The new powers in the Act contain a number of further safeguards not present in the current regime (to give just one example, a requirement that warrants be approved by a Judicial Commissioner: ss. 102-108 of the Act). Further safeguards will be contained in the new Code and arrangements made under the Code.

38. The IPT has ruled upon the compatibility of the current regime for acquiring and holding bulk personal datasets with the ECHR: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and ors* [2016] UKIPTrib 15_110-CH. It held on 17 October 2016 that the regime was not sufficiently accessible/foreseeable for the purposes of Article 8 ECHR prior to 12 March 2015, but was so thereafter. It adjourned issues of proportionality and a series of issues relating to the scope of EU law and, if applicable, compatibility with it for later determination. A hearing to determine those issues is scheduled for June 2017.

<u>Grounds of Resistance</u>

39. It is not the function of the Courts to decide hypothetical questions, which do not impact upon the parties before them, including questions that are premature: see e.g. *R(Rusbridger) v Attorney General* [2004] 1 AC 357 at [35] per Lord Hutton, *R v Secretary of State for the Home Department ex p Wynne* [1993] 1 WLR 115 at 119-120 per Lord Goff.

ECHR

40. Liberty's challenge to Parts 3, 4, 5, 6 and 7 of the Act under Articles 8 and 10 ECHR raises issues that are at this stage hypothetical and incapable of being resolved. They

will remain so until the relevant legal frameworks have been designed in their entirety, and are in force.

41. Liberty's assertion that the legal regimes under Parts 3, 5, 6 and 7 of the Act are not *"in accordance with the law"* (see SFG§§117, 132, 147, 162, 187 and 200) for the purposes of Articles 8 and 10 ECHR will only be capable of being addressed by examining those regimes in their entirety, including the statutory Codes of Practice and other material safeguards against abuse, and how those regimes operate:

    (1) The *"law"* for these purposes is to be understood in its substantive not formal sense. It encompasses not only statute, but also regulatory measures taken by regulatory bodies under independent rule-making powers delegated to them, and unwritten law. See e.g. *Sanoma Uitgevers BV v The Netherlands* [2011] EMLR 4 (Grand Chamber) at §83.

    (2) When assessing whether national law is accessible and foreseeable for the purposes of Articles 8 and 10, the relevant *"law"* will include published codes. See e.g. *Kennedy v United Kingdom* (2011) 52 EHRR 4 at §157 (the 2002 Interception of Communications Code of Practice was to be treated as part of the relevant *"law"* when assessing whether the interception regime pursuant to s.8(1) RIPA was *"in accordance with the law"*). See also *Liberty v UK* (2009) 48 EHRR 1 at §68 regarding the 2002 Code.

    (3) The question whether there are sufficient *"safeguards against abuse"* for the purposes of the foreseeability test under Articles 8 and 10 ECHR additionally requires examination of the internal practices and procedures of the relevant agencies operating the powers under the Act. "Below the waterline" procedures put in place by the agencies are relevant to whether the relevant regime gives adequate protection against arbitrary interference, provided that what is publicly disclosed sufficiently indicates the scope of the agencies' discretion and the manner of its exercise: see e.g. *Liberty and ors v GCHQ and ors* [2015] HRLR 2 at §§39-41, *Privacy International v SSFCO and ors* [2016] UKIPTrib 15_110-CH at §62.

42. The Claimants also assert that the relevant legal regimes are not *"necessary in a democratic society"* for the purposes of Articles 8 and 10 ECHR: see e.g. SFG§§117, 132, 147, 162, 187 and 200. That challenge also can only be assessed by examining the actual exercise of the powers concerned, in the light of the security threats that they are designed to address, and the measures and safeguards that will be put in place to strike an appropriate balance between the rights of the individual and the general interest.

43. Here, Liberty's challenge is brought almost a year before the earliest point at which any relevant provisions of the Act may come into force; several months before any Codes will be approved or published; well before any internal safeguards are made;

and thus, on any view, a long time before the question of any *exercise* of powers under the Act arises. That prematurity is only emphasised by the fact that Liberty's Grounds of Challenge wholly ignore the existence of Codes of Practice (even in a draft form for consultation), save to mention them in passing without considering their content and effect. It is not known with any certainty how the Codes may change following consultation, or what will be the ultimate form of the internal safeguards that will be put in place to govern the exercise of powers under the Act. In those circumstances, even if the Court proceeded to consider Liberty's claim by reference to the relevant provisions of the Act as elucidated by the draft Codes, that would still be premature because of the possibility of material differences in the final, published versions of the Codes (and any associated "below the waterline" arrangements).

EU law

44. The Defendants do not accept that the exercise of powers under Parts 5, 6 and 7 of the Act, and (in certain respects) Parts 3 and 4 of the Act falls within the scope of EU law at all. But even if it did, the same points relating to prematurity in the ECHR context apply equally to the Claimant's EU law challenge to the Act.

45. The Claimant's position, in purported reliance on *Watson*, is that EU law requires the relevant regimes to be *"legally binding under domestic law"* before they can be taken into account: see SFG §§88-89, relying on the CJEU's judgment at §117 and the Opinion of the Advocate-General in *Watson* at §§150-151. As to that:

    (1) The CJEU did not endorse the Advocate General's Opinion that EU law, unlike ECHR law, requires relevant safeguards to be legislative in nature and not contained in, e.g., statutory Codes of Practice. §117 of the CJEU's judgment in *Watson* refers to the *'the case-law cited in paragraph 109 of this judgment'*, i.e. the case law cited in paragraph 54 of joined cases C-293/12 and C-594/12 *Digital Rights Ireland*, which includes Strasbourg case law such as *Liberty and Others v. the United Kingdom; Rotaru v. Romania*, and *S. and Marper v. the United Kingdom*. This indicates that the CJEU, unlike the Advocate General, was not intending to depart from ECHR case law in this area.

    (2) In any event, the question whether a measure is *"legally binding under domestic law"* is, self-evidently, a question of national law, the answer to which can only be assessed by reference to the national legal order concerned.

    (3) As a matter of basic domestic public law, a statutory code of practice, to which decision-makers are required by statute to have regard, is legally binding. In accordance with public law principles of consistency and good administration, a decision-maker would be legally obliged to follow the code, unless he was able to show good reasons not to do so. See *R(Kambadzi) v Secretary of State for the Home*

Department [2011] UKSC 23, [2011] 1 WLR 1299 at §36 per Lord Hope, *R(Lumba) v Secretary of State for the Home Department* [2012] 1 AC 245 at §26 per Lord Dyson. The position is as stated by the Court of Appeal in *R(Nadarajah) v Secretary of State for the Home Department* [2004] INLR 139 at §54 (approved in *Kambadzi*):

> *"Our domestic law comprehends both the provisions of Schedule 2 to the Immigration Act 1971 and the Secretary of State's published policy, which, under principles of public law, he is obliged to follow."*

(4) In that regard, a person *"must"* have regard to Codes of Practice published under the Act when exercising any function to which the relevant Code relates. On that basis, the Codes of Practice constitute *"legally binding"* aspects of domestic law that must be taken into account in assessing the compatibility of the relevant legal regimes with EU law. It follows that, in circumstances where the Codes of Practice are still in draft, subject to consultation, and not expected to be finalised or approved for a number of months, the Claimant's EU law challenge to those regimes is premature on exactly the same basis as its ECHR challenge.

46. As to the prematurity of the challenge to Part 4 of the Act, the claim challenges a regime which is partially in force in so far as it relates to retention of communications data by CSPs, but which does not concern acquisition or use of such data by public authorities. 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.

47. As noted above, the prematurity of the claim in relation to both the ECHR and EU law issues is compounded by the fact that many of the same issues that arise in respect of Liberty's challenges to Part 5 and Part 6 (Chapters 1 and 3) of the Act are currently pending in the ECtHR in respect of challenges to the relevant predecessor legislation. Likewise, the IPT is presently seised of challenges to the predecessor legislation to Parts 6(2) and 7 of the Act, in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and ors* [2016] UKIPTrib 15_110-CH.

Conclusion

48. The proper course for Liberty to follow would be to intimate a challenge to the relevant powers once they are in operation, and their attendant legal regimes are fully implemented. It is only when the relevant legal frameworks are in place that a

Court can meaningfully assess the compatibility of those regimes with Article 8 and 10 ECHR and EU law.

49. That challenge should, moreover, be brought in the IPT, since that is the domestic tribunal set up precisely to consider to challenges of this type: it has in fact considered challenges to the various predecessor legal regimes to Parts 3, 5, 6 and 7 of the Act, as set out above; and it has well-established procedures and institutional expertise for the determination of the type of issues that arise in a claim of this sort. The Defendants' submission that this claim is premature is without prejudice to its ability, in due course, to contend that it ought also to be brought in a different forum.

50. For the reasons set out above, permission to apply for judicial review should be refused.

JAMES EADIE QC
GERRY FACENNA QC
JULIAN MILFORD
MICHAEL ARMITAGE