CO/2368/2016

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT
IN THE MATTER OF AN APPLICATION FOR JUDICIAL REVIEW

BETWEEN:

THE QUEEN on the application of
PRIVACY INTERNATIONAL

Claimant

-and-

INVESTIGATORY POWERS TRIBUNAL

Defendant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Interested Parties

SKELETON ARGUMENT OF THE INTERESTED PARTIES
For the Substantive Hearing on 8-9 December 2020

Time estimate: 1.5 days

References in square brackets are to the tab/page numbers in the hearing bundle served by the Claimant. References to the Claimant's skeleton argument are in the form "CS, §paragraph number".

Introduction

1. This claim concerns a judgment ("the Judgment") of the Investigatory Powers Tribunal ("IPT") dated 12 February 2016 on complaints by the Claimant and others about GCHQ's "Computer Network Exploitation" ("CNE") activities.[1] The Claimant's principal contention (the Claimant's "Issue 1") is that the IPT erred in law in its consideration of one of ten preliminary issues considered by the Tribunal in the

[1] *Privacy International and Greennet and others v Secretary of State for Foreign and Commonwealth Affairs and the Government Communications Headquarters* [2016] UKIP Trib 14_85-CH [**B/tab 5**].

Judgment, specifically regarding the construction of s.5 of the Intelligence Services Act 1994 ("ISA").[2]

2. In a carefully reasoned judgment the IPT gave general guidance about the scope of property warrants under s.5 ISA, concluding that such warrants had to be "as specific as possible" to enable to Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is "objectively ascertainable" (Judgment §47). For the reasons set out in detail at §§41-62 below, there was no error of law in that approach and the claim should be dismissed.

3. On 16 October 2019 the Claimant served draft Amended Statement of Facts and Grounds ("ASFG") [**A/tab 4**] on the Interested Parties, seeking to raise additional arguments concerning alleged contravention of Art. 8 of the European Convention on Human Rights ("ECHR"). The parties have agreed that the question of whether the Claimant should be granted permission to amend is to be considered at the substantive hearing. In its skeleton argument the Claimant now only seeks permission to amend on Art. 8 grounds in relation to the period *prior to* publication of the EI Code (the Claimant's "Issue 2").[3] For reasons set out at §§63-80 below, the Interested Parties submit that the new ground, even as now narrowed, lacks arguable merit. For that reason, and because of excessive and unjustified delay, permission to amend should be refused; however, if permission is granted, the new grounds should be dismissed.

Background

Computer Network Exploitation ('CNE')

4. CNE is a set of techniques through which an individual or organisation gains covert and remote access to equipment (including both networked and mobile computer devices) typically with a view to obtaining information from it.

5. There are a range of circumstances in which the agencies of the United Kingdom Intelligence Community ("UKIC") may be required to conduct this type of activity. CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE is used to secure valuable intelligence to enable the State to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

6. CNE operations may enable UKIC agencies to obtain communications and data of individuals who are engaged in activities which are criminal or harmful to national security in circumstances where it may otherwise be difficult or impossible to obtain

[2] "Issue 4" in the Judgment, which was addressed at §§31-47.
[3] CS, §1.2 and §85.

them. Other methods, such as interception, may be ineffective either because the intelligence sought may not have been communicated, or because a communication has been encrypted. The latter is increasingly prevalent. As the IPT observed in the Judgment, "*[t]he particular significance of the use of CNE is that it addresses difficulties for the Intelligence Agencies caused by the ever increasing use of encryption by those whom the Agencies would wish to target for interception.*" (§3) [4]

7. The Claimant asserts that "*CNE is potentially vastly more intrusive than telephone tapping.*" (CS, §72) The Interested Parties do not accept this as a fair characterisation. The most sensitive information held on a computer may still be communicated and be intercepted. Electronic communications are frequently encrypted and thus significantly protected from interception – indeed this is part of the reason why CNE is needed (see §6 above). The reality is that people entrust highly private information to encrypted electronic communication systems. There is no proper basis for the Claimant's claim that such information is in general terms any less private than that stored on computers or other devices. Furthermore, other systems of lawful surveillance (such as listening devices placed in people's homes) may acquire information that would be considered too sensitive even to record on a computer.[5] Similarly, all the material referred to by the Applicants (photographs, videos, passwords, banking details, passport details etc) would be potentially available by interception (subject to encryption) on Cloud storage which is increasingly used.[6]

8. At all material times, GCHQ's lawful basis for using CNE was either a property interference warrant granted pursuant to s.5 of the ISA, or an authorisation granted under s.7 of ISA.[7] The present claim is particularly concerned with s. 5 property interference warrants, by which the Secretary of State may authorise the "*taking…of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified…*" (s.5(2)). At the material time warrants issued pursuant to s.5 ISA were used to authorise CNE.[8]

---

[4] Ciaran Martin, 1st witness statement of 16 November 2015 [**A/tab 5**], §§11-12, 15-20, 30-31.
[5] Ciaran Martin, 1st statement [**A/tab 5**], §43.
[6] Ciaran Martin, 1st statement [**A/tab 5**], §44.
[7] Since 31 May 2018 CNE has been carried out pursuant to a targeted equipment interference warrant issued under Part 5 of the Investigatory Powers Act 2016 ("IPA") or, in the case of CNE carried out in "bulk", pursuant to a "bulk equipment interference warrant" issued under Part 6, Chapter 3 of the IPA. However, the Tribunal was considering the legality of arrangements which preceded the IPA, which is immaterial for present purposes.
[8] Although it is accurate to state, as C does at §§4.1-4.3, that a s.5 warrant may still be issued to authorise different kinds of interferences with property, it is <u>not</u> correct to state, as C does at CS, §4.4, that computer hacking may be so authorised. The activities described at CS, §4.4 would be likely to amount to an offence contrary to the Computer Misuse Act 1990. In such cases, the IPA is clear that an IPA warrant must be sought, in cases where "*there is a British Islands connection*": see IPA, s.13(1).

The IPT proceedings

9. The Claimant commenced proceedings in the IPT on 8 May 2014.[9] Separate proceedings were subsequently commenced by other complainants - "the GreenNet Claimants"[10] - in late June 2014.[11] The GreenNet Claimants are not parties to the present claim.

10. The Respondents to the claims were the Secretary of State for Foreign and Commonwealth Affairs ("SSFCA") and the Government Communication Headquarters ("GCHQ"), the Interested Parties in the present proceedings.

11. The claims alleged that GCHQ's use of CNE infringed Arts 8 and 10 of the ECHR.[12] The Claimant also made discrete arguments, introduced by amendment, which included that s.5 of ISA, which empowered the Secretary of State to issue a warrant in respect of "*such action as is specified in the warrant in respect of any property so specified*", did not permit the issuing of 'thematic' or 'class' warrants pursuant to s. 5 of ISA.[13] The terms 'thematic' and 'class' warrants are not found in section 5 itself. However, the Intelligence Services Commissioner (Sir Mark Waller), who at the material time had oversight over GCHQ's use of CNE, had referred in his 2014 Report to certain property interference warrants issued under section 5 which he considered arguably too broad or 'thematic'. The term 'class' authorisation was used by the Intelligence Services Commissioner to refer to s.7 authorisations, not s.5 warrants. The Intelligence Services Commissioner accepted that the agencies' interpretation of s.5 ISA was "*very arguable*" (see extract from the 2014 Report at Judgment, §33) but the Claimant argued before the IPT that the matters referred in the 2014 report demonstrated that s.5 ISA was being interpreted unlawfully.

12. The position of GCHQ and SSFCA in the IPT proceedings was that CNE was lawful both as a matter of domestic law and under the ECHR. There was a clear legal framework governing CNE activities, including the availability of warrants/authorisations under s.5 and s.7 ISA, supplemented by other provisions in statute (the Computer Misuse Act 1990, the Human Rights Act 1998, the Data Protection Act 1998, the Official Secrets Act 1989), relevant Codes of Practice, GCHQ's internal arrangements and mechanisms for oversight. That regime was both accessible and had a proper basis in domestic law. It provided for stringent safeguards if GCHQ wished to carry out CNE activities. It was also proportionate given the need for CNE to be carried out to protect the public from serious terrorist and other threats.

---

[9] Case number IPT 14/85.

[10] GreenNet Ltd, Riseup Networks Inc, Mango Email Service, Korean Progressive Network Jinobonet, Greenhost, Chaos Computer Club and Media Jumpstart Inc.

[11] Case numbers IPT 120-126/CH.

[12] The GreenNet Claimants also initially relied on Art. 1 of the First Protocol ("A1P1") to the ECHR, although the A1P1 claim was subsequently not pursued.

[13] §41C of Amended Grounds of Claim dated 19 May 2015. See the same paragraph in the Re-Amended Grounds of Claim dated 13 July 2015 [**B/tab 1/p.94/§41C**].

13. In relation to s.5 ISA the Interested Parties did not accept the Claimant's narrow interpretation and submitted that the Secretary of State was required to satisfy himself that the action to be authorised was both necessary and proportionate, thus placing a significant degree of control on the breadth of a given warrant.

14. The IPT adopted its established procedure to the claim, namely:[14]

    (a) where necessary, the IPT first holds a legal issues hearing in open session to determine such relevant pure issues of law as are in dispute between the parties, making assumptions as to significant facts in favour of claimants and reaching conclusions on that basis;

    (b) the IPT publishes its rulings (with reasons) on those pure issues of law;

    (c) the IPT then investigates the claim in closed session; and

    (d) as necessary,[15] the IPT applies its rulings on the pure issues of law to the facts that it has found following its closed session investigation of the claim.

15. As explained at §2 of the Judgment, the IPT conducted an open hearing on 1-3 December 2015 on preliminary issues of law. That represented stage (a) above. The constitution of the IPT consisted of two High Court Judges (Burton J and Mitting J as President and Vice President respectively) and three senior QCs[16].

16. Ten preliminary issues were before the IPT. The issues as agreed between the parties were set out in Appendix I to the Judgment, although they were subject to further reformulation by the IPT (Judgment, §10). Certain of the preliminary issues were phrased as questions of the proper interpretation of domestic law[17], while others were directed at establishing whether or not GCHQ had breached domestic/ECHR law.[18] The first issue which is material for present purposes ("Issue 4" as numbered in the Judgment) was a matter of statutory interpretation, namely:

    "What is the meaning of the words *'in respect of any property so specified'* for the purposes of the issue of a s.5 warrant?" (§34)

17. The issue was therefore <u>not</u> as described at CS, §20, but was reformulated by the IPT as above.

---

[14] As set out in its Procedural Ruling of 22 January 2003 in IPT/01/62 and IPT/01/77 at §173.
[15] Following its investigation the Tribunal may *e.g.* find that the respondents have not in fact undertaken any activities in relation to a claimant, with the result that the claim will be dismissed without the need to apply the rulings on the pure issues of law to any specific factual findings.
[16] Mr Robert Seabrook QC, Mr Charles Flint QC and The Hon Christopher Gardner QC
[17] See Issues 1, 3 and 4, 5: Judgment, §§12, 24, 34 and 48.
[18] See Issues 2 and 6 to 10: Judgment, §§21, 54, 60, 64, 71 and 84.

18. The other issue which is material for present purposes is Issue 9, which relates to the Claimant's application for permission to amend. It was:

> "*Did the s.5 regime prior to February 2015 accord with the Convention...?*" (§71)[19]

19. The factual basis against which the preliminary issues were considered comprised a combination of assumed facts and admissions, as set out at §5 and §9 of the Judgment.[20] However, as already noted, the IPT's function at the hearing was to construe s.5 ISA, rather than to determine whether any specific s.5 warrants were or were not lawful.

20. In its Judgment, the IPT set out its conclusions on the ten preliminary issues. These were summarised at §89. The IPT held, *inter alia*, that the regime for s.5 ISA warrants complied with Arts 8 and 10 ECHR, both before and after the introduction of a new Equipment Interference Code of Practice in February 2015 (§89(viii)-(ix)). In respect of the question concerning the meaning of the words *"in respect of any property so specified"* the IPT ruled as follows:

> *"Issue 4: A s.5 warrant is lawful if it is as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable, and it need not be defined by reference to named or identified individuals."* (§89(iv))

21. The IPT also concluded that *"[a] s.5 warrant which accords with the criteria of specification referred to in Issue 4 complies with the safeguards referred to in Weber (1) to (3), and consequently with Articles 8 and 10 in that regard."* (§89(vi))

22. As for Issue 9, the IPT held that "*[t]he s.5 regime prior to February 2015 was compliant with Articles 8/10.*" (§89(ix))

23. Following the Judgment, the IPT made "*no determination in favour*" in respect of each of the complainants, in accordance with the statutory provisions in s.68(4) of the Regulation of Investigatory Powers Act 2000 ('RIPA'), and notified them by letter dated 9 March 2016.

24. The present claim was commenced by a Claim Form lodged on 9 May 2016. On 17 June 2016 Lang J granted permission to apply for judicial review, and directed that there be a determination of a preliminary issue as to whether or not the IPT is amenable to judicial

---

[19] The period in question was from August 2009 to February 2015: Judgment, §73.

[20] The Claimant refers, at CS, §14, to a "*series of public disclosures, from June 2013 onwards, about the practices of the intelligence services.*" For the avoidance of doubt, the Respondents neither confirm nor deny any such alleged practices, nor any of the factual allegations made by the Claimant, save insofar as the Respondents made admissions in the underlying proceedings before the Tribunal.

review. The Divisional Court[21], and subsequently the Court of Appeal[22], held that it was not amenable, but that conclusion was overturned by the Supreme Court on 15 May 2019.[23]

25. On 16 October 2019 the Claimant served the draft ASFG on the Government Legal Department, solicitors for the Interested Parties. The parties have agreed that the question of whether the Claimant has permission to amend is to be heard alongside the existing permitted claim at a rolled-up hearing on the first available date after 10 February 2020 with a time estimate of 1.5 days (§3). As already noted, the Claimant now only seeks permission to amend in relation to the period *prior to* publication of the EI Code.[24]

Relevant legal provisions

The ISA (read with the CTA and the CMA)

GCHQ functions

26. By s. 3(1)(a) of the ISA, the functions of GCHQ at the material time[25] included the following:

> *"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."*

27. By s. 3(2) of the ISA, GCHQ's functions are only exercisable:

> "*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
> *(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
> *(c) in support of the prevention or detection of serious crime*."

28. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... that there are arrangements for securing that no information is obtained by GCHQ*

[21] *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin); [2017] 3 All E.R. 1127.
[22] *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWCA Civ 1868; [2018] 1 WLR 2572.
[23] *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219.
[24] The Claimant has reserved its position as to the period *after* publication of the EI Code until after the Grand Chamber of the ECtHR has given judgment in *Big Brother Watch v UK* (CS, §85).
[25] GCHQ's functions as defined in s.3(1) ISA were subject to certain amendments with effect from 13 February 2017, but none of the amendments are material for present purposes.

except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

Authorisation for equipment interference

s.5. warrants

29. By s. 5 of the ISA the Intelligence Services, including GCHQ, can apply for a warrant which provides specific legal authorisation for interferences with property and wireless telegraphy by them. Thus, at the material times[26], by s5(1) and (2) of the ISA:

> "*(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.*
>
> *(2) The Secretary of State may, on an application made by…GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State-*
>
> *(a) thinks it necessary for the action to be taken for the purpose of assisting…*
>
> *(iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and*
>
> *(b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;*
>
> *(c) is satisfied that satisfactory arrangements are in force under section 2(2)(a) of the* [Security Services Act 1989] *(duties of the Director-General of the Security Service), section 2(2)(a) above or section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements."*

30. When exercising his/her discretion and considering necessity and proportionality, the Secretary of State must take into account "*whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means*" (s.5(2A) ISA).

31. Pursuant to s. 5(3) of the ISA GCHQ may not be granted a s.5 warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

[26] Section 5 ISA was amended with effect from 13 February 2017. However, the amendments are not material for the purposes of this claim.

32. By s.6 of the ISA the procedure for issuing warrants and the duration of s. 5 warrants is addressed. In particular s.6(1) provides that a warrant shall not be issued save under the hand of the Secretary of State, unless it is a species of urgent case as set out in s.6(1)(b) or (d)[27].

33. In terms of duration, unless the warrant is renewed, it ceases to have effect at the end of the period of six months, beginning with the day on which it was issued (s. 6(2)) (save where the warrant was issued urgently and not under the hand of the Secretary of State in which case it lasts for 5 working days).

34. As to renewal, under s.6(3) of the ISA, if, before the expiry of the warrant, the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, it may be renewed for a period of six months.

35. By s. 6(4) of the ISA "*The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary*".

s.7 authorisations

36. In terms only of acts outside the British Islands, s.7 of the ISA also provides for the authorisation of such acts by the Intelligence Services including GCHQ. S.7(1) and 7(2) provide:

> "*(1) If, apart from this section; a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.*
>
> *(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom."*

37. Acts outside the British Islands include cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus (s. 7(9) ISA).[28]

---

[27] Those sub-sections provide:
(b) in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; ...
(d) in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of any of the specified officials.

[28] In addition ss.7(10)-(14) of the ISA recognise that it may be difficult, in certain circumstances to ascertain reliably the location of property and therefore provide, *inter alia*, that where acts are done in relation to property which is eg. mistakenly believed to be outside the British Islands, but which is done before the end of the 5th working day on which the presence of the property in the British Isles first becomes known, those acts will be treated as done outside the British Islands.

38. Under s. 7(4) of the ISA such an authorisation by the Secretary of State:

> "*(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;*
>
> *(b) may be limited to a particular person or persons of a description so specified; and*
>
> *(c) may be subject to conditions so specified."*

39. Consequently, the type of acts which may be covered by a s. 7 authorisation are broadly defined in the ISA and can clearly cover equipment interference outside the British Islands, where the tests in s. 7(3) of the ISA are satisfied.

40. In summary at the material time both s. 5 warrants and s.7 authorisations provided the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that the Intelligence Services were not civilly or criminally liable for such interferences.[29]

The IPT's conclusion in respect of the scope of s.5 ISA warrants

41. The IPT addressed the proper construction of the words "*in respect of any property so specified*" in s.5 ISA at §§31-47 of the Judgment.

42. The IPT first explained that questions about the breadth of s.5 warrants had first been raised in the 2014 report of the Intelligence Services Commissioner (see §§31-33). It noted that the term *"thematic warrants"* which was used in that report not only had *"no statutory basis"* (§31), but was also a description which *"does not appear to us to capture the reality of the issue which we have to decide."* Accordingly, at §34, the IPT reformulated the issue, which had previously asked whether "*s.5 ISA 1994 permit[s] the issue of a 'class' or 'thematic' warrant*" (Appendix I, Issue 2), as follows:

> "*What is the meaning of the words 'in respect of any property so specified' for the purposes of the issue of a s.5 warrant?*"[30]

43. Having set out the parties' submissions at §§35-36, the IPT explained, at §§37-46, why it was rejecting the narrow interpretation of s.5 ISA advanced by the Claimant. In summary it held that:

[29] Since 31 May 2018, the relevant powers have been those found in Parts 5 and 6 of the IPA: see footnotes 7 and 8 above.

[30] As originally formulated by the parties the issue was "*Does s.5 ISA 1994 permit the issue of a 'class' or 'thematic' warrant, i.e. a warrant authorising certain acts or types of acts in general rather than by reference to specified property or wireless telegraphy?*" (see Appendix I to the Judgment, Issue 2).

a. The 18th century cases about general warrants did not assist in the construction of an express statutory power of an intelligence service whose principal function involved furthering the interests of UK national security. The words in s.5 ISA had to be given their natural meaning in the context in which they were set (§37);

b. The issue as to whether the specification is sufficient in any particular case will be dependent on the particular facts of that case. The essential test was whether the actions and the property were sufficiently identified. As to that "*[t]he property should be so defined, whether by reference to persons or a group or category of persons, that the extent of the reasonably foreseeable interference caused by the authorisation of CNE in relation to the actions and property specified in the warrant can be addressed.*" (§38)

c. The issue was one of "*sufficiency of identification*". There was no need for the degree of particularisation required, for instance, by the words "*particular documents specified*" in the Evidence (Proceedings in Other Jurisdictions) Act 1975. (§39)

d. The IPT observed at §40 that "*what is of course important is what is put in the applications to the Secretary of State, so that he can exercise his discretion lawfully and reasonably.*" Further, "*[q]uestions of necessity and proportionality to be applied by the Secretary of State must relate to the foreseeable effect of the grant of such a warrant, and one of the matters to be considered is the effect and extent of the warrant in the light of the specification of the property in that warrant.*" (§41)

e. The word "*specified*" "*cannot have meant anything more restrictive than 'adequately described'*", in view of "*the width of meaning*" of the other terms which s.5 requires to be "*specified*", i.e. "*action*" and "*wireless telegraphy*" (§43-44).

f. The "*key purpose of specifying is to permit a person executing the warrant to know when it is executed that the action which he is to take and the property or wireless telegraphy with which he is to interfere is within the scope of the warrant.*" (§44) It was therefore not necessary for individual items of property to be identified (e.g. by name, location or owner), or for the property identified to be in existence at the date on which the warrant was issued (§45).

g. The meaning of s.5 ISA had been unchanged since its enactment. It was not changed with the amendment of s.7 ISA in 2001 to add GCHQ (§46).

44. The IPT's conclusion, at §47, was that:

> "*In our judgment what is required is for the warrant to be as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable.*"

45. The IPT's ruling on the construction of s.5 ISA in the separate "Conclusion" section of its Judgment at §89(iv) was in essentially identical terms to its conclusion at §47, although it also made clear (as had already been stated in §45(i)) that a s.5 warrant "*need not be defined by reference to named or identified individuals*."

Submissions

46. There is no merit in the suggestion that the IPT erred in law in its approach to the construction of s.5 ISA warrants. This is for the following reasons.

47. **First** the IPT's overarching approach was entirely appropriate, namely to look closely at the wording of s.5 in its particular statutory context; "*the words should be given their natural meaning in the context in which they are set*" (see §37). Adopting that approach the IPT was right to view the security context as special, with the following particular consequences:

    a. S.5 warrants must be capable of mitigating threats (including threats to national security) which are based on intelligence material and where it would be unrealistic to identify with complete precision what the property in question might be. Intelligence material, by definition, may be imprecise and particularly so where property interference abroad is envisaged.

    b. On a natural reading of s.5, the true drivers of control are the requirements of necessity and proportionality, which the Secretary of State is expressly directed to consider in s.5(2). Once it is appreciated that those fundamental safeguards are the core considerations when issuing a s.5 warrant, it is clear that the word "specified" is not designed to operate as a limiting or restricting criterion. Provided the property is described to a sufficient level of particularity so as to enable the Secretary of State to make a proper assessment of necessity and proportionality, all relevant statutory controls are satisfied.

    c. Accordingly, when applying the concept of "specified" in this particular legislative context, it is clear that this can encompass levels of particularity to a greater or lesser extent, depending on the state of knowledge in any given situation. As made clear by s.6 ISA, there may be a need to operate the warrant procedure very quickly in cases of extreme urgency and that has to be accommodated within the confines of the s.5 procedure. In those circumstances the IPT was right to conclude that "specified" cannot have meant anything more restrictive than "adequately described" (see §44).

    d. Allied to that, the concept of "specified" applies across a range of matters within s.5(1) including "*action as is specified*", "*property so specified*" and "*wireless telegraphy so specified*". Given the breadth e.g. of "*action*" and "*wireless telegraphy*"

as defined in s. 11(e) of ISA[31] 5(1), it would be illogical to adopt a narrow interpretation of "*property so specified*", particularly given the special context involved.

e. As to the Claimant's suggestion that recourse to Hansard is appropriate (see CS, §55), as recorded in the IPT judgment at §35(iv) both parties agreed at the hearing that this was of no assistance and in any event there is no ambiguity which would permit its use.

f. Nor is the meaning of s.5 ISA illuminated by reference to cases concerning the powers of tax inspectors using different statutory wording (see CS, §§53-54) or by reference to legislation from a context (proceedings of crime) which concerns neither national security nor the grant of warrants (CS, §56). The Claimant's reliance on the same underscores its failure to give weight to the contextual factors set out at (a)-(d) above (raised in the Detailed Grounds of Defence at §44 [**A/tab 8/p.151**] but nowhere addressed in the Claimant's skeleton argument). Indeed, the Claimant's argument with respect to *Ulster Bank* (CS, §§53-54) appears to amount to a submission that the definition of words in one statutory context necessarily translates to all other statutory uses of those words irrespective of context. That submission is obviously misconceived.

48. **Secondly**, it is important to recognise the nature and scope of the IPT's ruling about s.5 ISA. Properly characterised the IPT gave general guidance about the scope of warrants under s.5 ISA, making clear that for a warrant to be lawful it would be necessary:

    a. For the warrant to be "*as specific as possible*" and sufficiently so:

        i. To enable the Secretary of State to be satisfied as to legality, necessity and proportionality; and
        ii. To assist those executing the warrant; and

    b. For the property to be covered to be "*objectively ascertainable*".

49. The IPT expressly did not reach any conclusion about whether a given specification of property would or would not fall within the scope of s.5 ISA. That was consistent with its reformulation of the preliminary issue away from the question of whether "*s.5 ISA 1994 permit[s] the issue of a 'class' or 'thematic' warrant, i.e. a warrant authorising certain acts or types of acts in general rather than by reference to specific property or wireless telegraphy*" to a more open question of the construction of the words "*in respect of any property so specified*".

[31] Which could effectively amount to interference with an entire communications frequency or group of frequencies – see the definition in s.11(e) ISA with reference to s.19(1) of the Wireless Telegraphy Act 1949.

50. Given the IPT's careful conclusion that the legality of any given warrant would be "*dependent on the particular facts of that case*" (§38) and that "*what is of course important is what is put in the applications to the Secretary of State, so that he can exercise his discretion lawfully and reasonably*" (§40), it is unsurprising that the IPT did not choose to rule on overly-simplistic hypothetical examples (such as those set out in CS, Annex 1). The only reasonable response to those hypothetical examples would be "*it depends on all the circumstances*". The Claimant's attempts to challenge the IPT's ruling by asserting, for example, that it would permit a warrant authorising property interference over "*all mobile telephones in the United Kingdom*" or "*all computers used by anyone suspected by officials to be a member of a drug gang*" (ASFG, §31 [**A/tab 4/pp. 61-62**]) fail to engage with the IPT's finding that the legality of warrants is dependent on all of the circumstances. The examples provide none of the surrounding facts or intelligence assessments which the Secretary of State would be supplied with in order to assess legality, necessity and proportionality, nor any explanation of whether in those hypothetical scenarios it would have been possible to draw the warrant more narrowly.

51. **Thirdly**, the bright lines which are sought to be imposed by the Claimant through the language of "*property so specified*" have no proper or logical place in a regime of this kind.

52. In particular the touchstone for the lawfulness of the warrant cannot be whether or not the exercise of judgement is involved by those officials executing the warrant, as suggested by the Claimant (see eg. ASFG at §36 [**A/tab 4/p.63**] and CS, Annex 1). Even on the Claimant's own case, some judgement is necessary. So, for example, the Claimant accepts that property could be specified by reference to a geographical location (eg. 1 Acacia Ave – see their Annex 1). That is already a description i.e. a specification linked to property and it would not be clear which persons or which equipment would fall within it at the date of the warrant. The same could be said of a warrant which authorised the interference with computers in an internet café, which is also accepted as lawful by the Claimant[32]. By definition any such geographical descriptions have moved away from the concept of a named and identifiable individual and may require some degree of judgement when the warrant is executed. In addition, the Claimant accepts that it would be permissible to provide a description of the person eg. by colour of hair etc. (see 5th row at Annex 1) but that involves a judgement at the most basic level i.e. is this the person or not?

53. The Claimant also asserts that any group of persons specified in the warrant must be capable of being individually identified as at the date of the issue of the warrant, e.g. by list - see Annex 1. But again that is unrealistic. If the warrant provided for the interference with all mobile phones used by Provisional IRA members, on the Claimant's case it would be invalid as against any person who joined PIRA the day after the warrant was issued, or who was only identified as a member of PIRA by GCHQ for the first time the day after the warrant was issued. To construe s.5 in that way would be absurd and

[32] Transcript Day 1 (1 December 2015) at 85-86 [**B/tab 14/p.501**].

would defeat the central purpose of the legislation, namely the enabling of actions to be taken by the SIAs in the interests e.g. of national security or the prevention or detection of crime. If the Secretary of State has taken the decision that it is necessary and proportionate to interfere with all mobile phones used by PIRA, it would be extremely surprising if that warrant was unlawful simply because, as at the date of the warrant, not every person who might have their property interfered with could be named in a list.

54. Finally, it is to be noted that the overarching requirement for the property to be "*objectively verifiable*" was referred to by both parties before the IPT. That core test was suggested by the Claimant[33] and referred to as "common ground" by the Interested Parties[34], (without subsequent contradiction by Counsel for the Claimant, including in its skeleton argument for this hearing[35]). It is reflected in the test adopted by the IPT at §47. One of the express reasons why the IPT reached that conclusion reflected the Claimant's concern about questions of subjective judgement being left to the officer executing the warrant:

> "*The key purpose of specifying is to permit a person executing the warrant to know when it is executed that the action which he is to take and the property or wireless telegraphy with which he is to interfere is within the scope of the warrant.*" (§44)

55. Whilst the IPT did not accept the Claimant's narrow interpretation of s.5, its conclusion that the property to be covered must be "*objectively verifiable*" meets the point that too much might otherwise be left to the discretion of those executing the warrant.

56. **Fourthly**, the IPT's decision does not lead to the collapse or elision of the distinction between s.5 ISA warrants and s.7 ISA authorisations (contrary to CS, §§8 and 58). The distinction between s.5 and s.7 is that s.5 concerns entry on/interference with property or wireless telegraphy and s.7, on the other hand, relates to the "*authorisation of acts outside the British Islands*". Section 7 is necessarily broader because it covers a range of acts that may need to be authorised outside the UK, not only entry on/interference with property or wireless telegraphy. The distinction between that section and s.5 has not "collapsed" as a result of the IPT's judgment. It remains the case that s.7 permits a much wider range of activity to be authorised than s.5 and it is not possible to reason back from the breadth of s.7(4) to say that s.5(2), and the concept of "specified", should be construed narrowly.

57. Furthermore, when ss. 5 and 7 were enacted, s.5 related to GCHQ, but s.7 did not. It was not until 2001 that s.7 was amended to add the power for GCHQ to seek a s.7 authorisation abroad. Consequently, the contrast which the Claimant seeks to draw

[33] See, for instance, transcript Day 1, pp.112-113 [**B/tab 14/pp.507-8**].
[34] Transcript, Day 2, p. 139, lines 23-24 [**B/tab 15/p.576**].
[35] This description of the common ground between the parties before the IPT was set out in the Detailed Grounds of Defence of 20 December 2019 at §51 [**A/tab 8/p.153**]. The Claimant has not disputed it.

between the language of s.5 and s.7 did not exist so far as GCHQ was concerned at the date of the passage of RIPA (see §36(ii) and §37 of the Judgment)[36] – which is the relevant date for assessing Parliamentary intention.

58. If there is a contrast to be drawn between different kinds of warrants, the more revealing exercise is to consider the level of specificity required by s.8(1) of the RIPA when dealing with interception warrants. As noted by the IPT, section 8(1) requires an interception warrant to name or describe either one person as the interception subject[37] or a single set of premises as the premises in relation to which the interception is to take place (see Judgment at §32). By contrast Parliament has chosen to use much broader language in s.5 ISA with a greater level of flexibility as to the "*property so specified*".

59. **Fifthly**, the IPT correctly concluded that the Eighteenth-Century cases about general warrants were not useful in the interpretation of s.5 ISA. Instead the IPT held that "*the words should be given their natural meaning in the context in which they are set*" (see §37). There was no error of law in that approach.

    a. The context in *Huckle v Money*[38] and *Wilkes v Wood*[39], which the Claimant describes as "*[t]he most important cases for present purposes*" (CS, §38), was very different. It concerned political libels[40]; these were not national security threats of the kind for which a s.5 ISA warrant is issued.

    b. There was no requirement on the Minister granting the warrants in *Huckle* and *Wilkes* to consider whether they were necessary and proportionate. The delegation of a power to search the property of a widely defined class is of course of more concern where there is no check on the grant of that power by reference to whether it is necessary and proportionate to grant it. Section 5 ISA does not have that problem – it may allow interference with the property of a wide class, but only if the Minister has concluded that it is necessary and proportionate to do so.

    c. Further, the vice with the general warrants in *Wilkes* was that the warrant was so wide that they provided "*a discretionary power…to messengers to search wherever their suspicions may chance to fall*" (see 498). Properly considered *Wilkes* and *Huckle* are not authorities for the proposition that a warrant cannot relate to a wide class; rather it must not confer so wide a discretion on those carrying out the warranted activity to search wherever they choose. However, that is not what the IPT's ruling does. Rather, it makes clear that the property covered by a warrant must be "*objectively ascertainable*" precisely to ensure that no such wide discretion is conferred.

---

[36] As to the suggestion that recourse to Hansard is appropriate – see CS, §7.2 – see §47(e) of this skeleton argument.
[37] A person includes any organisation and any association or combination of persons (as defined in s. 81 RIPA).
[38] (1763) 2 Wilson 205, 95 ER 768
[39] (1973) Lofft 1, 98 ER 489
[40] In a publication called The North Briton - *Wilkes* at 490 *Huckle* at 768, final paragraph.

60. **Finally**, it is a mischaracterisation of the IPT's decision to assert that the IPT "*rejected the relevance of the principle of legality*" as asserted at CS, §8; see also CS, §65. Nowhere in the operative paragraphs setting out its reasoning do the IPT state that the principle of legality does not apply to matters of national security. Nor did it treat the need for clarity when authorising interferences with property as a "*historical artefact*" (contrary to CS, §50). That was not what the IPT decided. Whilst the IPT did (rightly) conclude that the Eighteenth century common law cases about general warrants were "*not a useful or permissible aid to construction*" of the express statutory powers given to the intelligence agencies in the ISA (see §37), it was no part of the IPT's careful reasoning to conclude that the principle of legality could never have any application in the national security sphere.

61. In any event, the principle of legality is a rule of statutory interpretation which means that fundamental rights cannot be overruled by general or ambiguous statutory words. As stated by Lord Dyson in *AJA v Commissioner of Police of the Metropolis* [2014] 1 WLR 285, it is an important tool of statutory interpretation and "*no more than that*". As he made clear "*when an issue of statutory interpretation arises, ultimately the question for the court is always to decide what Parliament intended*" (see §28). The courts have therefore reiterated, on numerous occasions, that the principle has no role where the intention of Parliament is clear from the ordinary or natural meaning of a statutory provision, read in in the context of the legislative scheme as a whole.[41]

62. For these reasons, there was no error of law in the IPT's carefully reasoned ruling on the interpretation of s.5 ISA.

Amended grounds based on Art. 8 ECHR

63. The question of whether the Claimant should be granted permission to amend to pursue new Art.8 grounds is to be considered on a rolled-up basis at the hearing of this claim. The Supreme Court made clear in *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219 that permission to apply for judicial review of a decision of the IPT should only be granted in cases "*raising points of general significance*"(1259D; §112). Furthermore, the status of the IPT, which has "*apparently equivalent status and powers to those of the High Court*" was "*to be respected and taken into account...by the careful regulation of the court's power to grant or refuse permission for judicial review.*" (1255H, §99).[42] The Claimant's new Art. 8 arguments lack merit for reasons set

[41] See *R (Gillan) v Metropolitan Police Commissioner* [2006] 4 All ER 1041, per Lord Bingham at §15, *R (Richards) v Teesside Magistrates Court* [2016] 2 All ER 950, Beatson LJ and *McE v Prison Service of Northern Ireland & Ors* [2009] 1 AC 908 per Lord Hope at 61-62.

[42] These statements were made in Lord Carnwath's judgment on the first issue before the Supreme Court, namely whether section 67(8) RIPA 2000 ousts the High Court's supervisory jurisdiction to quash a judgment of the Tribunal for error of law. Baroness Hale, Lord Kerr and Lord Lloyd Jones agreed with Lord Carnwath on that issue, and his judgment on it was therefore that of the majority (see 1225E; and 1268A; §147).

out at §§64-79 below, and are also brought after an excessive delay without justification (see §80 below). However, importantly they also seek to challenge the Judgment of the IPT not on pure issues of statutory interpretation (such as the s.5 thematic warrant ground addressed above) but on the IPT's judgement as an expert Tribunal, with particular experience and depth of understanding of the *Weber* criteria to be applied when considering whether a system of surveillance is "*in accordance with law*". This is a further reason, in addition to the lack of merit in the grounds, and the delay in bringing them, why the position of the Interested Parties is that permission should be refused to expand the claim at this late stage as proposed. Further and in any event, if and insofar as permission is granted, the new grounds should be dismissed.

Lack of substantive merit

64. **First**, the Claimant seeks to argue that the s.5 ISA warrantry regime was unlawful prior to February 2015 because "*almost nothing about the arrangements governing the use of CNE was publicly acknowledged*": see CS, §§76-80. The Interested Parties do not accept this criticism. The IPT addressed the question of the applicability of the Property Code to CNE as follows at Judgment, §81:

> "it was quite clear that at least since 1994 the powers of GCHQ have extended to computer interference (under s.3 of ISA). It was thus apparent in the public domain that there was likely to be interference with computers, hacking being an ever more familiar activity, namely interference with property by GCHQ (and see in particular the 1990 Hansard references in paragraph 18(iii) above), and that if it occurred it would be covered by the Property Code...."

65. This analysis was entirely correct:

    a. GCHQ's powers to conduct CNE had indeed been clear since the enactment of s.3(1) of ISA in 1994, which provided: "*...[GCHQ's] functions shall be- (a) to monitor* ***or interfere with*** *electromagnetic, acoustic and other emissions* ***and any equipment producing such emissions****...****and provide information derived from or related to*** *such emissions* ***or equipment****...*" (emphasis added)[43].

    b. Indeed, the fact that "*the security services*" carried out "*hacking*" had been explicitly discussed in Parliament as early as 1990, during the debate over the Computer Misuse Bill (see Judgment, §§18(iii) and 81). Indeed, the Claimant realistically appears to accept that intelligence services' use of CNE before the publication of the EI Code was obvious, but says that "*[i]t was not at all obvious that they were doing so* **lawfully**…" (CS, §79; emphasis added);

---

[43] Section 3(1) ISA was amended, on 13 February 2017, to insert the words "*make use of*" after "*monitor*" and before "*or interfere with*".

c. The Property Code made clear that it "*provide[d] guidance on entry on, **or interference with, property or with wireless telegraphy** by public authorities under **section 5 of the Intelligence Services Act 1994**...*" (§1.2, emphasis added) CNE clearly involves interference with property, and so fell within the clear terms of the Property Code. The Property Code therefore met the condition of sufficient clarity necessary for it to be foreseeable that it governed CNE.

66. Thus the Claimant's contentions that "*there was nothing in [the Property Code] to suggest it was being treated by the intelligence services as applicable to CNE*", that it "*would have been no more than a guess*" that the Property Code applied to CNE, and that "*to an external observer it would have been at least as likely that there was no Code of Practice governing CNE at all*", and CS, §§76-80 more generally, are unarguable.

67. **Secondly,** the Claimant also contends that the safeguards in the Property Code were not "*adequate*" (CS, §12). No particulars of the alleged inadequacy are given in the Claimant's skeleton, which may suggest a further narrowing of the application to amend. However, the ASFG stated that "*the provisions of the Property Code were not compliant with the fourth, fifth and sixth Weber criteria. They made no clear provision as to the procedures to be followed in examining, using and storing data obtained through CNE, the precautions to be taken when communicating such data, or the circumstances in which such data would be deleted or destroyed*." (ASFG, §49B.2)

68. These criticisms – if they are maintained – are without arguable merit. They notably appear to proceed on the incorrect basis that the Property Code was to be read in isolation, rather than as one part of a wider system of law and guidance. They also do not address the specific provisions of the Property Code itself. Furthermore, they are in effect criticisms of the judgement of an expert Tribunal as to what in the national security surveillance context amount to adequate safeguards to avoid arbitrary interferences (see §63 above). The Interested Parties submit, on a proper analysis, that the s.5 warrantry regime was in accordance with law before February 2015 for the following reasons.

69. In relation to **examination, use and storage of data**:

a. Pursuant to the Property Code, guidance was given as to the handling of material obtained through property interference. §9.3 of the Code stated as follows:

"*Each public authority must ensure that arrangements are in place for the **secure handling, storage and destruction of material** obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, **must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998** and any relevant codes of practice produced by individual authorities relating to the **handling and storage of material**.*" (emphasis added)

In addition, the Code stated at §9.7 that, in relation to the intelligence services:

> "***The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the ... 1994 Act***." (emphasis added)

In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

70. In relation to **communication/disclosure to other parties**:

a. Any information emanating from equipment interference could be used by GCHQ only in accordance with s.19(2) of the Counter-Terrorism Act 2008 ("CTA") as read with the statutory definition of GCHQ's functions (in s. 3 of the ISA) and only insofar as proportionate under s.6(1) of the Human Rights Act 1998 ("HRA").

b. Pursuant to the Data Protection Act 1998 ("DPA") (which was in force at the material times), GCHQ was not exempt from an obligation to comply with the seventh data protection principle, which provided:

> " *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."[44]

Accordingly, if GCHQ obtained any information as a result of any property interference which amounted to personal data, it was obliged to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

c. Any disclosure eg. deliberately in breach of the "arrangements" for which provision is made in s.4(2)(a) of the ISA would be a criminal offence under s.1(1) of the Official Secrets Act 1989 ("OSA") which could attract imprisonment of up to two years.

d. Further a member of the intelligence service will commit an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the ISA read with s.1(1) of that Act). Conviction may lead to imprisonment of up to 3 months.

[44] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

e. Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 at §§191-194).

f. Finally any disclosure of such information had to satisfy the constraints imposed in s. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

71. In relation to **destruction**:

a. The 2010/2014 Property Code addressed the destruction of material at §9.3 and stated as follows :

> "*Each public authority must ensure that arrangements are in place for the secure handling, storage and* ***destruction*** *of material obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.*" (emphasis added)

In addition, the Code stated at §9.7 that, in relation to the Intelligence Services:

> "***The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions…"*** (emphasis added)

b. In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

c. Pursuant to the DPA, GCHQ was not exempt from an obligation to comply with the fifth data protection principle, which provided:

> "*Personal data processed*[45] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …"*

Accordingly, when GCHQ obtained any information as a result of any property interference which amounted to personal data, it was obliged not to keep that data for longer than is necessary having regard to the purposes for which they had been obtained and were being retained/used.

[45] The term "*processing*" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

72. In addition, further substantive safeguards were set out in "*below the waterline arrangements*" and contained in the oversight mechanisms of the Intelligence Services Commissioner, the Intelligence and Security Committee of Parliament and the IPT (see Judgment, §74(ii)(a)-(b), §§76-77). They were also of relevance when considering whether overall the pre-February 2015 regime contained effective safeguards against abuse.

73. In those circumstances, if the criticisms at ASFG, §49B.2 are still maintained – notwithstanding the absence of reference to them in the Claimant's skeleton – the fourth to sixth *Weber* requirements were plainly met for the pre-February 2015 regime. The Judgment's expert conclusion to that effect is not arguably open to criticism.

74. **Thirdly**, the Claimant contends that the fact that the draft EI Code published in February 2015 contained enhanced safeguards, not found in the Property Code, rendered the Property Code unlawful (CS, §§81-83). That is not accepted. In *R (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin); [2019] HRLR 16 the Divisional Court (Haddon-Cave LJ and Swift J) rejected the argument that an enhancement of safeguards in a code of practice (in that case regulating police use of automated facial recognition technology) would render pre-existing safeguards inadequate.[46] They held that "*the possibility (or even the likelihood) of such improvement is not evidence of present deficiency*" (§93). The IPT applied the same reasoning in its Judgment at §82:

> "*...a conclusion that procedural requirements or the publication of them can be improved (i) does not have the necessary consequence that there has prior thereto been insufficient compliance with Weber (4) to (6) and (ii) does not constitute such a material non-compliance as to create a contravention of Article 8.*"

75. Contrary to the Claimant's suggestion, it was this essential logic, rather than a concern not to disincentivise improvement by the intelligence services of their policies, which was at the heart of the IPT's reasoning. Nor does the fact that a policy could reveal more without damaging the interests of national security automatically render a policy not "*in accordance with law*". The touchstone for lawfulness remains the tests of foreseeability and accessibility set out in *Weber*. For reasons already explained, the Property Code complied with those tests.

76. **Finally**, despite stating that this ground is now limited to the period "*prior to publication of the Equipment Interference Code*" (CS, §1.2), the Claimant still seeks to identify unlawfulness in the s.5 ISA warrantry regime in the period after February 2015 – at least for as long as the Code in force was the *draft* EI Code (CS, §67).[47]

---

[46] The judgment of the Divisional Court was reversed on other grounds by the Court of Appeal: *R (Bridges) v Chief Constable of South Wales* [2020] EWCA 1058; [2020] HRLR 16. However, this conclusion of the Divisional Court was neither challenged nor reversed on appeal.

[47] NB the date given at CS, §67 for the publication of the draft EI Code is not correct. It was published in February 2015, not February 2016 (as the Claimant elsewhere correctly notes: CS, §10 and §17). The Claimant repeats the error at CS, §84. There are further errors in the Claimant's skeleton as regards

77. The IPT addressed this issue in their Judgment at §64:

> *"The E I Code applies to both s.5 and s.7...., and,* ***as Mr Jaffey accepted****, the Respondents, having publicly accepted that they are acting and will act in accordance with the draft Code,* ***are as a matter of public law bound by the Code*** *... in relation to s.5, during the period prior to its being fully approved by Parliament..."* (emphasis added)

78. The IPT's analysis involved no error of law. Indeed, as the IPT recorded, it was *accepted* by counsel for the Claimant. What is important is that the published draft E I Code bound the Interested Parties as a matter of public law. It accordingly set out legally enforceable standards which gave the s.5 warrantry regime sufficient basis in domestic law for it to be "*in accordance with law*". The fact that it was in draft, and had not yet been approved by Parliament, did not alter its binding nature. The Interested Parties could not, for instance, have raised as a defence in any complaint to the IPT about an alleged breach of the draft E I Code the fact that it was in draft and not yet approved by Parliament. The Claimant's reliance on those factors puts form over substance.

79. For these reasons, the Claimant's new Art. 8 arguments are without arguable merit. This is sufficient reason in and of itself to refuse permission to amend as sought.

Delay

80. Furthermore, the new Art. 8 grounds were not raised until more than *three years* after the claim was first issued and until more than *four years* after the period of alleged unlawfulness (pre-February 2015). The delay has been so substantial that the s.5 warrantry regime for CNE is no longer even in force (having been replaced by Part 5 and Part 6, Chapter 3 of the Investigatory Powers Act 2016 on 31 May 2018). Furthermore, the justification put forward by the Claimant for the delay (CS, §13) is incoherent and misleading. Even if (which is not accepted) the fact that it was unclear whether the IPT was amenable to judicial review could justify raising only domestic law, not ECHR grounds, the Claimant did *in fact* raise Art. 8 grounds at the outset, albeit different ones to those now pursued (see §§40-49 of the Grounds as issued [**A/tab 3/pp.30-33**]). In truth, the Claimant appears to have no justification at all for seeking to expand its Art. 8 case so late in the proceedings.

Conclusion

81. There was no error of law in the IPT's carefully reasoned ruling on the interpretation of s.5 ISA and the claim should be dismissed. Further, for reasons both of lack of substantive merit, and delay, the Court is invited to refuse the Claimant permission to

---

subsequent developments with the EI Code. The EI Code was laid before Parliament in November 2015 and was approved in January 2016 (Judgment, §5). C omits reference to the November 2015 laying before Parliament, and wrongly gives January "2017" as the date on which it received Parliamentary approval (CS, §§67 and 84).

amend its grounds to argue an Art. 8 claim. Alternatively, if permission is granted, the Court should dismiss those grounds.

24 November 2020 **SIR JAMES EADIE QC**
RICHARD O'BRIEN