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

SUMMARY GROUNDS OF DEFENCE OF THE INTERESTED PARTIES

[References in square brackets are to the page numbers in the JR bundle served by the Claimant.]

Introduction

1. On 12 February 2016 the Investigatory Powers Tribunal (IPT) gave judgment in the linked 'Privacy' and 'Greennet' complaints[1] both of which related to GCHQ's "Computer Network Exploitation" ('CNE') activities.

2. After receiving detailed pleadings and evidence and after hearing three days of oral argument in December 2015, the IPT set out its conclusions on a number of preliminary issues concerning the lawfulness of CNE, including its compatibility with Arts. 8 and 10 ECHR. 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[2]. Following the preliminary issues judgment in February 2016, 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.

3. In these judicial review proceedings, the Claimant contends that:

---

[1] IPT/14/85/CH and IPT/14/120-126/CH.
[2] Mr Robert Seabrook QC, Mr Charles Flint QC and The Hon Christopher Gardner QC

a. the IPT is a body which is amenable to judicial review;
b. the IPT erred in law when it considered the proper interpretation of s.5 of the Intelligence Services Act 1994 ('the ISA') which provides for the issuing of warrants for the interference with, *inter alia*, property in the United Kingdom where that is necessary for the purpose of assisting GCHQ in carrying out its statutory functions (including eg. for the protection of national security); and, more generally and contrary to the IPT's conclusion, that the statutory scheme, for the issuing of s. 5 ISA warrants, as interpreted by the IPT, is incompatible with Art. 8 ECHR[3].

4. The Interested Parties submit that neither of these points are properly arguable.

Section 67(8) of RIPA 2000

5. Section 67(8) of RIPA 2000 provides as follows:

> *"Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court."*

6. Five submissions are made. **First,** the express language of s.67(8) is clear and unambiguous:

   a. Parliament has made plain that all aspects of the IPT's decision-making shall not be challenged whether by way of appeal or by way of questioning in any court.
   b. That wording was evidently intended to, and on its face and natural meaning does, exclude the application of judicial review to decisions of the IPT. That judicial review jurisdiction falls within the final words of this section, in contradistinction and in addition to an appeal which is also precluded.
   c. The words in parenthesis also support that conclusion. They make clear that it matters not whether a challenge is on the grounds of excess of jurisdiction or decisions within jurisdiction (to the extent that those concepts remain of relevance post-*Anisminic*[4]). The section is thus evidently also intended to, and does, exclude all such public law challenges.

7. **Secondly,** the Supreme Court's judgment in *R (A) v Director of Establishments of Security Service* [2010] 2 AC 1 (see copy attached), supports that interpretation. The Supreme

---

[3] For the avoidance of doubt, none of the Claimant's factual allegations about the use of and/or the intrusiveness of CNE activities should be assumed in these proceedings. An accurate summary of what has and has not been confirmed publicly by GCHQ appears in §5 and §9 of the IPT's judgment [C/178 & 180-181] and in the witness statements of Mr Ciaran Martin, Director General of Cyber Security at GCHQ[3] (copies of which are attached herewith). As is evident from those materials, a number of assumed facts in the IPT proceedings were the subject of the Neither Confirm Nor Deny (NCND) principle. In addition, it has been the practice of successive Governments to adopt a NCND stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government - and in the IPT proceedings that included the document which appears at C/350-354 of the Claimant's bundle.

[4] [1969] 2 AC 147

Court considered whether RIPA (and in particular s.65(2)(a)) had conferred exclusive jurisdiction on the IPT to hear claims under s.7(1) of the Human Rights Act 1998 ('the HRA') against any of the intelligence services. (Lord Brown gave the judgment of the Court, with whom all other members of the Supreme Court agreed.)

8. Having set out the *"legislative provisions most central to the arguments"*, which included s.67(8) of RIPA 2000 (see §3 and §5), the Supreme Court emphasised the specialist nature of the IPT regime. At §14, they stated:

> *"There are, moreover, powerful other pointers in the same direction. Principal amongst these is the self-evident need to safeguard the secrecy and security of sensitive intelligence material, not least with regard to the working of the intelligence services. It is to this end, and to protect the "neither confirm nor deny" policy (equally obviously essential to the effective working of the services), that the Rules are as restrictive as they are regarding the closed nature of the IPT's hearings and the limited disclosure of information to the complainant (both before and after the IPT's determination). There are, however, a number of counterbalancing provisions both in RIPA and the Rules to ensure that proceedings before the IPT are (in the words of section 69(6)(a)) "properly heard and considered". Section 68(6) imposes on all who hold office under the Crown and many others too the widest possible duties to provide information and documents to the IPT as they may require. Public interest immunity could never be invoked against such a requirement. So too sections 57(3) and 59(3) impose respectively upon the Interception of Communications Commissioner and the Intelligence Services Commissioner duties to give the IPT "all such assistance" as it may require. Section 18(1)(c) disapplies the otherwise highly restrictive effect of section 17 (regarding the existence and use of intercept material) in the case of IPT proceedings. And rule 11(1) allows the IPT to "receive evidence in any form, and [to] receive evidence that would not be admissible in a court of law". **All these provisions in their various ways are designed to ensure that, even in the most sensitive of intelligence cases, disputes can be properly determined. None of them are available in the courts. This was the point that so strongly attracted Dyson LJ in favour of B's case in the court below. As he pithily put it, ante, p 19, para 48:***
>
> > *"It seems to me to be inherently unlikely that Parliament intended to create an elaborate set of rules to govern proceedings against an intelligence service under section 7 of the 1998 Act in the IPT and yet contemplated that such proceedings might be brought before the courts without any rules."* (emphasis added)

9. At §§21-24 the Supreme Court then considered whether s.65(2)(a), in providing for the exclusive jurisdiction of the IPT in respect of certain types of claims against the intelligence agencies , constituted an impermissible ouster of the ordinary jurisdiction of the courts. They concluded that it did not. That was because:

   a. RIPA, the HRA and the Civil Procedure Rules had come into force at the same time as part of a *"single legislative scheme"*.
   b. The exclusive jurisdiction given to the IPT, which was not a court of inferior jurisdiction, but was a specialist tribunal with special procedures apt for the subject matter in hand, did not take away a pre-existing common law right to the court and so did not amount to an ouster of the ordinary jurisdiction of the courts;

c. Parliament had not ousted judicial scrutiny of the acts of the intelligence services, it had simply *allocated* that scrutiny to the IPT.

10. At §§23-24, the Supreme Court specifically distinguished the relevant regime from that which had operated in *Anisminic* and also considered the import of s.67(8) of RIPA. They stated:

> *"Nor does Anisminic assist A. The ouster clause there under consideration purported to remove any judicial supervision of a determination by an inferior tribunal as to its own jurisdiction. Section 65(2)(a) does no such thing.* ***Parliament has not ousted judicial scrutiny of the acts of the intelligence services; it has simply allocated that scrutiny*** *(as to section 7(1)(a) HRA proceedings)* ***to the IPT.*** *Furthermore, as Laws LJ observed, ante, p 13, para 22:*
>
> > ***"statutory measures which confide the jurisdiction to a judicial body of like standing and authority to that of the High Court, but which operates subject to special procedures apt for the subject matter in hand, may well be constitutionally inoffensive. The IPT ... offers ... no cause for concern on this score."***
>
> ***True it is that section 67(8) of RIPA constitutes an ouster (and, indeed, unlike that in Anisminic, an unambiguous ouster) of any jurisdiction of the courts over the IPT. But that is not the provision in question here and in any event, as A recognises, there is no constitutional (or article 6) requirement for any right of appeal from an appropriate tribunal.***
>
> *24 The position here is analogous to that in Farley v Secretary of State for Work and Pensions (No 2) [2006] 1 WLR 1817 where the statutory provision in question provided that, on an application by the Secretary of State for a liability order in respect of a person liable to pay child support, "the court ... shall not question the maintenance assessment under which the payments of child support maintenance fall to be made". Lord Nicholls of Birkenhead, with whom the other members of the committee agreed, observed, at para 18:*
>
> > *"The need for a strict approach to the interpretation of an ouster provision ... was famously confirmed in the leading case of Anisminic ... This strict approach, however, is not appropriate if an effective means of challenging the validity of a maintenance assessment is provided elsewhere. Then section 33(4) is not an ouster provision. Rather, it is part of a statutory scheme which allocates jurisdiction to determine the validity of an assessment and decide whether the defendant is a 'liable person' to a court other than the magistrates' court.""* (emphasis added)

11. The Supreme Court was therefore satisfied that the IPT was a judicial body of like standing and authority to the High Court and one which operated subject to a highly specialist regime. The IPT is not a body which Parliament ever intended would be subject to judicial review.

12. **Thirdly**, if any further support were needed for that conclusion, it is to be found in the following other aspects of the IPT regime, in addition to those emphasised by the Supreme Court at §14 of *A* (see §8 above):

a. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA) and the President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA). The fact that High Court Judges sit in the IPT is a *"powerful factor"* in ascertaining whether in substance it should be subject to judicial review (see *R v Cripps ex p Muldoon* [1984] QB 68, *R (Cart) v Upper Tribunal* [2011] QB 120 and *R (Woolas) v Parliamentary Election Court* [2012] QB 1 at §33).

b. When the Tribunal considers any complaints under s.65(2)(a) and 65(2)(b) it is the duty of the Tribunal to:

> *"apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review"* (see s.67(2) and, to same effect, s. 67(3) of RIPA).

It is therefore clear that Parliament has allocated such public law challenges exclusively to the IPT and has instructed the IPT to act as though it were the High Court in an application for judicial review.

13. Thus, having regard to its constitution, jurisdiction and powers, the IPT cannot properly be regarded as inferior to the High Court such that it is amenable to judicial review – see *Cart* per Laws LJ at §§40, 69-70.

14. **Fourthly,** the IPT regime has been endorsed by the ECtHR in *Kennedy v United Kingdom* (2011) 52 EHRR 4, in which the extensive jurisdiction of the IPT and the considerable restrictions applied by it in order to safeguard secret information, were found to be compatible with Article 6 ECHR. Nothing was said in that case to indicate any Article 6 concern about the exclusivity of its jurisdiction. On the contrary, the ECtHR specifically noted at §77 of its judgment that there was *"no appeal from a decision of the IPT"*.

15. **Fifthly,** it is to be noted that legislative changes to introduce a right of appeal are currently under specific consideration by Parliament in the Investigatory Powers Bill, which had its first and second readings in the House of Commons on 19 May 2016. Clause 208 of the Bill provides as follows:

> *"208 Right of appeal from Tribunal*
> *(1) After section 67 of the Regulation of Investigatory Powers Act 2000 insert –*
>
> *"67A Appeals from the Tribunal*
>
> ***(1) A relevant person may appeal on a point of law against any determination of the Tribunal of a kind mentioned in section 68(4) or any decision of the Tribunal of a kind mentioned in section 68(4C).***
>
> *(2) Before making a determination or decision which might be the subject of an appeal under this section, the Tribunal must specify the court which is to have jurisdiction to hear the appeal (the "relevant appellate court").*
>
> *(3) This court is whichever of the following courts appears to the Tribunal to be the most appropriate –*
> *(a) the Court of Appeal in England and Wales,...*

(5) An appeal under this section –
(a) is to be heard by the relevant appellate court, but
(b) may not be made without the leave of the Tribunal or, if that is refused, of the relevant appellate court.

(6) The Tribunal or relevant appellate court must not grant leave to appeal unless it considers that—
(a) the appeal would raise an important point of principle or practice, or
(b) there is another compelling reason for granting leave..."
(emphasis added)

16. The Explanatory Notes to Clause 208 state as follows at §§516-518:

> "*Currently there is no domestic route of appeal from a decision or determination of the Investigatory Powers Tribunal, with Claimant's having to pursue appeals to the European Court of Human Rights if they wish to challenge a decision. This clause amends RIPA to introduce a domestic appeal route from decisions and determinations of the Investigatory Powers Tribunal on a point of law, to the Court of Appeal in England and Wales.... Regulations will detail the criteria to be considered by the Investigatory Powers Tribunal when determining the relevant appellate court.*
>
> *Where there is a point of law, the decision on whether to grant permission to appeal will be taken by the Investigatory Powers Tribunal in the first instance. If the Tribunal refuses to grant permission to appeal, this decision may be reviewed by the appeal court.*
>
> *The Tribunal or appellate court must not give permission to appeal on a point of law unless the appeal would raise an important point of principle or practice or they consider that there are other compelling reasons to grant permission to appeal, such as that it would be in the wider public interest.*"

17. Had it been the case that decisions of the IPT were already challengeable on a point of law by way of judicial review, then these amendments would be unnecessary.

18. In addition, it is to be noted that the proposed basis upon which appeals from the IPT will proceed in future is by applying what has been termed the "*second tier appeals criteria*" test (see *Cart* in the Supreme Court [2012] 1 AC 663 at §52 per Lady Hale and §129 per Lord Dyson) i.e. it is not any error of law which will justify an appeal, but only one falling within the restricted tests set out in Clause 208(6). That supports the proposition that Parliament intends the statutory regime to be a complete code (with no room for the application of judicial review) i.e. Parliament sets the limits on the jurisdiction of the IPT and any challenges from it.

19. The Claimant's Grounds advance no properly arguable points capable of meeting the analysis above. In particular:

    a. It is wrong to suggest that the ouster clause in *Anisminic* was "*almost identical*" to s.67(8) of RIPA 2000. The Supreme Court expressly considered that point and concluded that they were not the same - the clause in *Anisminic* was "*ambiguous*" in contrast to s.68(7). Not only is the scope of the two clauses very different, but context is important. In *Anisminic*, the House of Lords was considering an ouster

clause in respect of an inferior tribunal, where there was no suggestion that it exercised powers on a par with the High Court. For the reasons given by the Supreme Court in *A*, the IPT's position is fundamentally different.

b. The IPT is not an *"inferior tribunal"* (see §55 of the Claimant's Grounds). Nor is there anything in the offensive and inaccurate suggestion that it is *"staffed by individuals of lesser ability"* (see §56) than Judges of the High Court.

c. It follows therefore that none of the concerns set out at §56 of the Claimant's Grounds arise here - the IPT is a specialist tribunal of like standing and authority to the High Court and as such is *"constitutionally inoffensive"* (see Laws LJ in *A*[5] (consistent with what he stated at §40 of *Cart* - cited with approval by the Supreme Court at §23 of *A*).

Did the IPT err in law in its conclusions on the scope of s.5 ISA warrants?

20. Without prejudice to the matters set out above, there is no merit in the suggestion that the IPT erred in law in its approach to the construction of s.5 ISA warrants.

21. **First**, it is mischaracterisation of the IPT's decision to assert that the IPT *"rejected a principle of fundamental constitutional importance"* i.e. the "principle of legality" - as asserted at §9, §37 and §57 of the Claimant's Grounds. 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. 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 of the judgment), 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.

22. 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). That is precisely what the IPT did in this instance, as is evident from §§37-47 of the judgment.

23. **Secondly**, the IPT was right when it 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*[6] and *Wilkes v Wood*[7] was very different. It concerned political libels[8]; these were not national security threats of the kind for which a s.5 ISA warrant is issued.

---

[5] [2009] EWCA Civ 24

[6] (1763) 2 Wilson 205, 95 ER 768

[7] (1973) Lofft 1, 98 ER 489

[8] in a publication called The North Briton - *Wilkes* at 490 *Huckle* at 768, final paragraph

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.

24. **Thirdly**, the IPT's decision does not lead to the collapse of the distinction between s.5 ISA warrants and s.7 ISA authorisations. The IPT accepted the submission of the Interested Parties that s.7 ISA is a different provision which relates to the *"authorisation of acts outside the British Islands"* i.e. s.7 is broad because it covers a range of acts that may need to be authorised outside the UK and therefore does not fall to be directly contrasted with s.5 ISA[9]. That is clear, not least from the fact that only in 2001 was s.7 amended to add the power for GCHQ to seek a s.7 authorisation abroad and consequently there was no such contrast between s.5 and s.7 of the ISA so far as GCHQ were concerned at the date of the passage of RIPA (see §36(ii) and §37 of the IPT judgment)[10].

25. **Fourthly**, the Claimant accepts that it is not necessary for the intelligence agencies to identify a named individual or a specific item of property at the time of applying for the warrant. Whilst the Claimant submitted to the IPT that *"identification cannot depend upon the belief suspicion or judgment of the officer acting under the warrant"* (see §35(iii) of the IPT decision), 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 at A/39). 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. In addition, the Claimant accepts that it would be permissible to describe the person eg. 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?

26. In those circumstances, the IPT was correct to conclude its analysis by stating that it is necessary for the warrant to be as specific as possible in relation to the property to be covered, 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 (see §47). Contrary to the Claimant's submissions at §31 that does not mean eg. that it would be permissible to authorise property

[9] The language of s7: uses *"acts of a description specified"* in s7.4 which does suggest that things can be specified by description. That on no view implies that *'specified'* can only be by reference to particular, identified property (eg. A's computer).

[10] As to the suggestion that recourse to Hansard is appropriate – see §36(g) of the Claimant's Grounds, 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.

interference over *"all mobile telephones in the United Kingdom"* or *"all computers used by anyone suspected to be a member of a drug gang"*. As made clear by the Interested Parties at the hearing, whilst a warrant covering *"all mobile phones in Birmingham"* could be sufficiently specified, it would be unlikely to be either consistent with necessity or proportionality or with GCHQ's statutory obligations (see §36(iii) of the judgment at C/195).

27. **Finally**, it is important to be clear about the proper limits of the IPT's actual decision. The IPT judgment gives general guidance about the scope of warrants under s.5 ISA. However, it was careful to make plain that the lawfulness of the warrant in any particular case would be dependent on the particular facts of that case (see §38). It also made clear that any warrant should be *"as specific as possible"* in relation to the property covered by the warrant (§47). The day to day oversight for such matters rests with the Intelligence Services Commissioner who brought this issue to public attention in his 2014 Report and who himself has made five recommendations about the use of what might be termed thematic warrants, as set out at [C/279]. In particular, the Commissioner has indicated that any warrants which might be considered to be thematic should be highlighted in the list which is provided for his selection during his inspections. In those circumstances, given the cautious approach of the IPT and the day to day oversight provided by the Commissioner, there is no proper basis on which the High Court could or should be drawn into this arena. It is plainly not the case that there is no independent oversight of the powers in s.5 ISA as alleged in §§44 and 46 of the Claimant's Grounds.

Article 8 ECHR

28. At §§40-49 of the Grounds the Claimants assert that Art. 8 of the ECHR does not permit the issuing of a warrant authorising modern forms of electronic surveillance without prior authorisation by a Court. These points are not only without merit, but were not raised before the IPT in the CNE proceedings. In the IPT proceedings in *Liberty/Privacy* [2015] HRLR 2, in which the main judgment was handed down on 5 December 2014 (i.e. approx 15 months ago), the IPT held that prior judicial authorisation was not required (see §151). Even if the IPT was amenable to judicial review (which it is not), they cannot justify a challenge to the IPT's February 2016 judgment in the CNE proceedings.

29. In addition, it is incorrect to suggest that the ECtHR judgment in *Szabo & Vissy v Hungary* (Application 37128/14, 12 January 2016) makes clear that such authorisation is required. At §77 the ECtHR stated:

> *"The Court recalls that in Dumitru Popescu (cited above, §§70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and others, cited above, §§42 and 55). **The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation** (see Kennedy, cited above, §167)."* (emphasis added)

Protective Costs Order

30. If, contrary to the above submissions, the Court grants permission, the Court will need to be satisfied that this judicial review is of general public importance and that the public interest requires these issues to be resolved, if a protective costs order is to be made (see *R (Corner House Research) v Secretary of State for Trade and Industry* [2005] 1 WLR 2600 at §74). It is submitted that in light of (1) the careful guidance given in the IPT judgment about s.5 ISA warrants and (2) the ongoing oversight by the Commissioner in this specific area (see §32 above), that criterion is not satisfied. Further and/or alternatively if a PCO is made limiting the Claimant's costs to £15,000 (as has been proposed), then there should be a reciprocal cap on the Interested Parties' costs liability at the same level.

27 May 2016

JAMES EADIE QC
KATE GRANGE

A

The Law Reports

Appeal Cases

Volume 2

B

C

Supreme Court

Regina (A) *v* Director of Establishments of the Security Service

[2009] EWCA Civ 24

[2009] UKSC 12

D

2009 Oct 19, 20; Dec 9

Lord Phillips of Worth Matravers PSC, Lord Hope of Craighead DPSC, Lord Brown of Eaton-under-Heywood, Lord Mance, Lord Clarke of Stone-cum-Ebony JJSC

Tribunal — Statutory — Investigatory Powers Tribunal — Security Service refusing consent for publication by former member of service of material describing his work for service — Former member claiming judicial review on ground refusal E *breaching Convention right to freedom of expression — Whether claim "proceedings against any of the intelligence services" or against Crown — Whether Investigatory Powers Tribunal "appropriate court or tribunal" in which proceedings to be brought — Whether tribunal having exclusive jurisdiction — Human Rights Act 1998 (c 42), s 7(1)(a) — Regulation of Investigatory Powers Act 2000 (c 23), s 65(2)(a)(3)(a)*

F The claimant, a former senior member of the Security Service, wrote a book about his work with the service and wished to publish it. He was however bound by strict statutory and contractual obligations as well as duties of confidentiality and he was required to obtain the consent of the Director of Establishments of the Security Service before publication. The director refused consent to the publication of parts of the book. The claimant commenced judicial review proceedings in the High Court to challenge the director's refusal on the ground, inter alia, that it was contrary to his G right to freedom of expression under article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, as scheduled to the Human Rights Act 1998[1]. The director contended that the High Court had no jurisdiction to entertain

[1] Human Rights Act 1998, s 7: see post, Supreme Court judgments, para 3.

Sch 1, Pt I, art 6(1): "In the determination of his civil rights and obligations . . . everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public H may be excluded from all or part of the trial in the interests of . . . national security in a democratic society . . ."

Art 10: "1. Everyone has the right to freedom of expression. This right shall include freedom to . . . impart information and ideas without interference by public authority . . . 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security . . ."

the claim in so far as it alleged breach of article 10 since that was a claim under section 7(1)(a) of the 1998 Act and, by virtue of section 65(2)(a) of the Regulation of Investigatory Powers Act 2000[2], the Investigatory Powers Tribunal ("IPT") was "the only appropriate tribunal" in relation to proceedings under section 7(1)(a) of the 1998 Act brought against one of the intelligence services, and it was the "appropriate court or tribunal" within the meaning of section 7(1)(a) for a claim under article 10. The judge rejected that contention and ruled on a preliminary issue that section 65(2)(a) of the 2000 Act only excluded the jurisdiction of other tribunals but did not exclude the court's jurisdiction. The Court of Appeal allowed the director's appeal and held that the High Court had no jurisdiction to entertain the article 10 claim and that it should go before the IPT.

On appeal by the claimant—

Held, dismissing the appeal, that, on a true construction, section 65(2)(a) of the 2000 Act conferred on the IPT exclusive jurisdiction to hear claims under section 7(1)(a) of the 1998 Act against any of the intelligences services, and section 65(3)(a) of the 2000 Act did not limit that exclusive jurisdiction only to hearing proceedings arising out of the exercise of one of the regulated investigatory powers in the 2000 Act; that, since the relevant provisions of the 2000 Act, the 1998 Act and the Civil Procedure Rules had come into force at the same time as part of a single legislative scheme, the exclusive jurisdiction given by section 65(2)(a) to the IPT, which was not a court of inferior jurisdiction but operated subject to special procedures apt for the subject matter in hand, did not take away a pre-existing common law or statutory right of recourse to the court and so did not amount to an ouster of the ordinary jurisdiction of the courts but merely represented the allocation of part of the court's jurisdiction to the IPT; that, since the 2000 Act and the Rules made thereunder contained provisions which were designed to ensure that, even in the most sensitive of intelligence cases, disputes before the IPT were properly heard and considered and there was a sufficient measure of flexibility and adaptability in the IPT's rules and procedures to enable it to provide as much information to the claimant as possible consistently with national security interests, hearing the claimant's complaint in the IPT would not necessarily involve a breach of the claimant's article 6 right to a fair trial; and that, accordingly, the claimant had to bring his claim in the IPT (post, paras 13–18, 21–24, 26, 30, 38, 39–40, 42–43, 50).

Barraclough v Brown [1897] AC 615, HL(E) and *Farley v Secretary of State for Work and Pensions (No 2)* [2006] 1 WLR 1817, HL(E) applied.

Pyx Granite Co Ltd v Ministry of Housing and Local Government [1960] AC 260, HL(E); *Anisminic Ltd v Foreign Compensation Commission* [1969] 2 AC 147, HL(E) and *R v Shayler* [2003] 1 AC 247, HL(E) considered.

Decision of the Court of Appeal, post, p 5; [2009] EWCA Civ 24; [2009] 3 WLR 717; [2009] 3 All ER 416 affirmed.

The following cases are referred to in the judgments of the Supreme Court:

Anisminic Ltd v Foreign Compensation Commission [1969] 2 AC 147; [1969] 2 WLR 163; [1969] 1 All ER 208, HL(E)

Applications Nos IPT/01/62 and IPT/01/77 (unreported) 23 January 2003, Investigatory Powers Tribunal

Barraclough v Brown [1897] AC 615, HL(E)

Deposit Protection Board v Dalia [1994] 2 AC 367; [1994] 2 WLR 732; [1994] 2 All ER 577, HL(E)

Dimond v Lovell [2000] QB 216; [1999] 3 WLR 561; [1999] 3 All ER 1, CA

Esbester v United Kingdom (1993) 18 EHRR CD 72

Farley v Secretary of State for Work and Pensions (No 2) [2006] UKHL 31; [2006] 1 WLR 1817; [2006] 3 All ER 935, HL(E)

[2] Regulation of Investigatory Powers Act 2000, s 65: see post, Court of Appeal judgments, para 5.

A *Hanlon v The Law Society* [1981] AC 124; [1980] 2 WLR 756; [1980] 2 All ER 199, HL(E)
Pyx Granite Co Ltd v Ministry of Housing and Local Government [1960] AC 260; [1959] 3 WLR 346; [1959] 3 All ER 1, HL(E)
R v Kansal (No 2) [2001] UKHL 62; [2002] 2 AC 69; [2001] 3 WLR 1562; [2002] 1 All ER 257, HL(E)
R v Shayler [2002] UKHL 11; [2003] 1 AC 247; [2002] 2 WLR 754; [2002] 2 All ER
B 477, HL(E)
R (Al-Skeini) v Secretary of State for Defence (The Redress Trust intervening) [2007] UKHL 26; [2008] AC 153; [2007] 3 WLR 33; [2007] 3 All ER 685, HL(E)
R (Ullah) v Special Adjudicator [2004] UKHL 26; [2004] 2 AC 323; [2004] 3 WLR 23; [2004] 3 All ER 785, HL(E)
Sunday Times v United Kingdom (No 2) (1991) 14 EHRR 229
Wilson v First County Trust Ltd (No 2) [2003] UKHL 40; [2004] 1 AC 816; [2003]
C 3 WLR 568; [2003] 4 All ER 97, HL(E)

The following additional cases were cited in argument before the Supreme Court:

Ghaidan v Godin-Mendoza [2004] UKHL 30; [2004] 2 AC 557; [2004] 3 WLR 113; [2004] 3 All ER 411, HL(E)
Jersild v Denmark (1994) 19 EHRR 1

D The following cases are referred to in the judgments of the Court of Appeal:

Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109; [1988] 2 WLR 805; [1988] 3 All ER 545, Scott J and CA; [1990] 1 AC 109; [1988] 3 WLR 776; [1988] 3 All ER 545, HL(E)
R v Lord Chancellor's Department, Ex p Nangle [1991] ICR 743; [1992] 1 All ER 897, DC
R v Shayler [2002] UKHL 11; [2003] 1 AC 247; [2002] 2 WLR 754; [2002] 2 All ER
E 477, HL(E)

No additional cases were cited in argument before the Court of Appeal.

The following additional cases, although not cited, were referred to in the skeleton arguments before the Court of Appeal:

F *AEI Rediffusion Music Ltd v Phonographic Performance Ltd* [1999] 1 WLR 1507; [1999] 2 All ER 299, CA
Anisminic Ltd v Foreign Compensation Commission [1969] 2 AC 147; [1969] 2 WLR 163; [1969] 1 All ER 208, HL(E)
Leech v Deputy Governor of Parkhurst Prison [1988] AC 533; [1988] 2 WLR 290; [1988] 1 All ER 485, HL(E)
R (G) v Immigration Appeal Tribunal [2004] EWCA Civ 1731; [2005] 1 WLR 1445; [2005] 2 All ER 165, CA
G *R (Sivasubramaniam) v Wandsworth County Court* [2002] EWCA Civ 1738; [2003] 1 WLR 475; [2003] 2 All ER 160, CA
Tanfern Ltd v Cameron-MacDonald (Practice Note) [2000] 1 WLR 1311; [2000] 2 All ER 801, CA

APPEAL from Collins J

H By a claim form issued on 13 November 2007, the claimant, A, a former member of the Security Service, claimed judicial review of the decision of the defendant, the Director of Establishments of the Security Service, taken on 14 August 2007, to refuse the claimant permission to publish a manuscript relating to his work for the Security Service on the grounds that the defendant's decision had been unreasonable, vitated by bias and a breach of

the claimant's right to freedom of expression under article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. On a preliminary issue raised by the defendant that the court had no jurisdiction to deal with the claim, Collins J on 4 July 2008 found in favour of the claimant that the Investigatory Powers Tribunal did not have exclusive jurisdiction but granted the director permission to appeal.

By an appellant's notice filed on 25 July 2008 the director appealed on the grounds that (1) the judge had erred in concluding that section 65(2)(a) of the Regulation of Investigatory Powers Act 2000 did not confer exclusive jurisdiction upon the Investigatory Powers Tribunal to hear claims under section 7(1)(a) of the Human Rights Act 1998 which were brought against the Security Service; and (2) while the judge had correctly recognised that both the Administrative Court and the Investigatory Powers Tribunal had jurisdiction to hear the complaints of unreasonableness and bias he had then erred in concluding that the Administrative Court was the appropriate forum in which those complaints should be heard.

The facts are stated in the judgment of Laws LJ.

Philip Havers QC and *Jason Coppel* (instructed by *Treasury Solicitor*) for the director.

Only the Investigatory Powers Tribunal has jurisdiction to hear a claim of breach of article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. A claim pursuant to article 10 is a claim within the meaning of section 7(1)(a) of the Human Rights Act 1998 and is assigned exclusively to the "appropriate court or tribunal". The "appropriate court or tribunal" is ordinarily by force of CPR r 7.11 "any court". But where the claim is brought against any of the intelligence services, it is by force of section 65(2)(a) of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Tribunal. The High Court accordingly has no jurisdiction in the matter.

Gavin Millar QC and *Guy Vassall-Adams* (instructed by *Bindmans LLP*) for the claimant.

Section 7(2) of the 1998 Act defines "the appropriate court or tribunal" as such court or tribunal as is determined by rules. By CPR r 7.11(2), the court or tribunal is simply "any court" which would include the Administrative Court. By using the words "to be the only appropriate tribunal", section 65(2)(a) of the 2000 Act assigns a class of case which would otherwise have been heard by another tribunal to the Investigatory Powers Tribunal. Section 65(2)(a) of the 2000 Act provides that claims which before 2 October 2000 would have been entertained in the earlier specialist tribunals must now, so far as they assert a violation of Convention rights, be brought before the Investigatory Powers Tribunal. However, where an article 10 claim has been properly brought as an autonomous action in the Administrative Court, that court is the "appropriate court" by force of CPR r 7.11, and section 65(2)(a) of the 2000 Act is not engaged. Where the director has refused to grant authorisation to a claimant to make a disclosure, the claimant is entitled to rely on article 10 of the Convention in judicial review proceedings in the Administrative Court: see *R v Shayler* [2003] 1 AC 247.

The proceedings are in substance brought against the Crown, and therefore are not "proceedings against any of the intelligence services"

A within the meaning of section 65(3)(a) of the 2000 Act. Therefore section 65(2)(a) is not engaged and the Administrative Court is "the appropriate court or tribunal" for the purposes of section 7 of the 1998 Act: see *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, CA and HL(E).

Havers QC in reply.

B The fact that the Crown is the legal personality behind the Security Service does not take the Security Service out of section 65(3)(a) of the 2000 Act, nor therefore out of section 65(2)(a).

The court took time for consideration.

18 February 2009. The following judgments were handed down.

C

LAWS LJ

Introduction

1 This is an appeal, with permission granted by the judge below, against the decision of Collins J given in the Administrative Court on 4 July 2008 to the effect that the Administrative Court possesses jurisdiction to hear the D respondent claimant's claim against the appellant defendant alleging a violation of article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. I will refer to the respondent as the claimant.

2 The claimant is a former member of the Security Service. He has written and desires to publish a manuscript which, as Collins J put it, E "contains inter alia a description of his work for the service". Bound as he is by a strict duty of confidentiality, he may not publish such material without the authority of the appellant (defendant in the proceedings), who is the Director of Establishments of the Security Service and to whom I will refer as the director.

3 The claimant applied for the director's consent to publish, which F was refused. Thereafter on 13 November 2007 the claimant lodged an application in the Administrative Court for permission to bring judicial review proceedings to challenge the director's refusal of consent. He claimed that the refusal violated his right of free expression guaranteed by article 10 of the Convention, and was unreasonable and vitiated by bias. On the same day, 13 November 2007, Collins J gave directions including orders to protect the identities of the claimant and the proposed defendant (there is G however no difficulty in the way of naming the defendant/appellant, by reference to his office: so much was done in Collins J's substantive judgment now under appeal). On being served with the proceedings the director asserted that the Administrative Court had no jurisdiction to entertain the claim of violation of Convention rights. On 12 March 2008 Collins J granted judicial review permission and directed a preliminary hearing on the H jurisdiction issue raised by the director. On 15 June 2008 Collins J conducted the preliminary hearing, and his reserved judgment sub nom *A v B (Investigatory Powers Tribunal: Jurisdiction)* [2008] 4 All ER 511, by which he decided the jurisdiction issue in favour of the claimant, was delivered on 4 July 2008 and as I have indicated is now the subject of this appeal.

4 The director's contention is that by force of section 65(2)(a) of the Regulation of Investigatory Powers Act 2000, to which I will come directly, the only judicial entity having jurisdiction to entertain the article 10 claim is the Investigatory Powers Tribunal (the "IPT"), which was established by section 65(1) of the 2000 Act. The High Court and thus the Administrative Court therefore has none.

Statutory materials

5 I should first set out the following provisions of the 2000 Act.

"65 *The tribunal*

"(1) There shall, for the purpose of exercising the jurisdiction conferred on them by this section, be a tribunal consisting of such number of members as Her Majesty may by Letters Patent appoint.

"(2) The jurisdiction of the tribunal shall be— (a) to be the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 in relation to any proceedings under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights) which fall within subsection (3) of this section; (b) to consider and determine any complaints made to them which, in accordance with subsection (4), are complaints for which the tribunal is the appropriate forum . . . (d) to hear and determine any other such proceedings falling within subsection (3) as may be allocated to them in accordance with provision made by the Secretary of State by order.

"(3) Proceedings fall within this subsection if— (a) they are proceedings against any of the intelligence services . . .

"(4) The tribunal is the appropriate forum for any complaint if it is a complaint by a person who is aggrieved by any conduct falling within subsection (5) which he believes— (a) to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any postal service, telecommunications service or telecommunication system; and (b) to have taken place in challengeable circumstances or to have been carried out by or on behalf of any of the intelligence services.

"(5) Subject to subsection (6), conduct falls within this subsection if (whenever it occurred) it is— (a) conduct by or on behalf of any of the intelligence services . . .

"66 *Orders allocating proceedings to the tribunal*

"(1) An order under section 65(2)(d) allocating proceedings to the tribunal— (a) may provide for the tribunal to exercise jurisdiction in relation to that matter to the exclusion of the jurisdiction of any court or tribunal; but (b) if it does so provide, must contain provision conferring a power on the tribunal, in the circumstances provided for in the order, to remit the proceedings to the court or tribunal which would have had jurisdiction apart from the order."

"67 *Exercise of the tribunal's jurisdiction*

"(1) Subject to subsections (4) and (5), it shall be the duty of the tribunal— (a) to hear and determine any proceedings brought before them by virtue of section 65(2)(a) or (d); and (b) to consider and determine any complaint or reference made to them by virtue of section 65(2)(b) or (c).

A "(2) Where the tribunal hear any proceedings by virtue of section 65(2)(a), they shall apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review."

"68 *Tribunal procedure*

"(1) Subject to any rules made under section 69, the tribunal shall be B entitled to determine their own procedure in relation to any proceedings, complaint or reference brought before or made to them.

"(2) The tribunal shall have power— (a) in connection with the investigation of any matter, or (b) otherwise for the purposes of the tribunal's consideration or determination of any matter, to require a relevant commissioner appearing to the tribunal to have functions in relation to the matter in question to provide the tribunal with all such C assistance (including that commissioner's opinion as to any issue falling to be determined by the tribunal) as the tribunal think fit . . .

"(4) Where the tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of section 69(2)(i)) shall be confined, as the case may be, to either— D (a) a statement that they have made a determination in his favour; or (b) a statement that no determination has been made in his favour."

"(6) It shall be the duty of the persons specified in subsection (7) to disclose or provide to the tribunal all such documents and information as the tribunal may require for the purpose of enabling them— (a) to exercise the jurisdiction conferred on them by or under section 65; or (b) otherwise to exercise or perform any power or duty conferred or E imposed on them by or under this Act."

(Section 68(7) then sets out a list of persons. The first, at section 68(7)(a), is "every person holding office under the Crown".) Section 69 empowers the Secretary of State to make rules regulating the IPT's exercise of its jurisdiction and other matters. Then section 70:

F "*Abolition of jurisdiction in relation to complaints*

"(1) The provisions set out in subsection (2) (which provide for the investigation etc of certain complaints) shall not apply in relation to any complaint made after the coming into force of this section.

"(2) Those provisions are— (a) section 5 of, and Schedules 1 and 2 to, the Security Service Act 1989 (investigation of complaints about the Security Service made to the tribunal established under that Act); G (b) section 9 of, and Schedules 1 and 2 to, the Intelligence Services Act 1994 (investigation of complaints about the Secret Intelligence Service or GCHQ made to the tribunal established under that Act); and (c) section 102 of, and Schedule 7 to, the Police Act 1997 (investigation of complaints made to the Surveillance Commissioners)."

H 6 I must next give some account of the Investigatory Powers Tribunal Rules 2000 (SI 2000/2665) made by the Secretary of State pursuant to section 69 of the 2000 Act.

7 Rule 2 of the 2000 Rules defines "section 7 proceedings" as "proceedings under section 7(1)(a) of the Human Rights Act 1998 in relation to which the tribunal is the only appropriate tribunal by virtue of

section 65(2)(a) of the [2000] Act". By rule 3, the Rules are applied to section 7 proceedings. There follows a series of provisions elaborating special procedures clearly fashioned to accommodate the particular considerations, not least those of national security, which are likely to arise in such proceedings. Notable among them is rule 6, headed "Disclosure of information", part of which is in these terms:

"(1) The tribunal [sc the IPT] shall carry out their functions in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.

"(2) Without prejudice to this general duty, but subject to paragraphs (3) and (4), the tribunal may not disclose to the complainant or to any other person: (a) the fact that the tribunal have held, or propose to hold, an oral hearing under rule 9(4); (b) any information or document disclosed or provided to the tribunal in the course of that hearing, or the identity of any witness at that hearing; (c) any information or document otherwise disclosed or provided to the tribunal by any person pursuant to section 68(6) of the [2000] Act (or provided voluntarily by a person specified in section 68(7)); (d) any information or opinion provided to the tribunal by a commissioner pursuant to section 68(2) of the [2000] Act; (e) the fact that any information, document, identity or opinion has been disclosed or provided in the circumstances mentioned in sub-paragraphs (b) to (d).

"(3) The tribunal may disclose anything described in paragraph (2) with the consent of: (a) in the case of sub-paragraph (a), the person required to attend the hearing; (b) in the case of sub-paragraphs (b) and (c), the witness in question or the person who disclosed or provided the information or document; (c) in the case of sub-paragraph (d), the commissioner in question and, to the extent that the information or opinion includes information provided to the commissioner by another person, that other person; (d) in the case of sub-paragraph (e), the person whose consent is required under this rule for disclosure of the information, document or opinion in question.

"(4) The tribunal may also disclose anything described in paragraph (2) as part of the information provided to the complainant under rule 13(2), subject to the restrictions contained in rule 13(4) and (5)."

8 I should refer also to rules 9 and 13 of the Rules. Rule 9 is headed "Forms of hearing and consideration". It provides:

"(1) The tribunal's power to determine their own procedure in relation to section 7 proceedings and complaints shall be subject to this rule.

"(2) The tribunal shall be under no duty to hold oral hearings, but they may do so in accordance with this rule (and not otherwise).

"(3) The tribunal may hold, at any stage of their consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses.

"(4) The tribunal may hold separate oral hearings which: (a) the person whose conduct is the subject of the complaint, (b) the public authority against which the section 7 proceedings are brought, or (c) any other

A person specified in section 68(7) of the [2000] Act, may be required to attend and at which that person or authority may make representations, give evidence and call witnesses.

"(5) Within a period notified by the tribunal for the purpose of this rule, the complainant, person or authority in question must inform the tribunal of any witnesses he or it intends to call; and no other witnesses may be called without the leave of the tribunal.

B "(6) The tribunal's proceedings, including any oral hearings, shall be conducted in private."

Rule 13 is headed "Notification to the complainant". It provides:

"(1) In addition to any statement under section 68(4) of the [2000] Act, the tribunal shall provide information to the complainant in accordance

C with this rule.

"(2) Where they make a determination in favour of the complainant, the tribunal shall provide him with a summary of that determination including any findings of fact.

"(3) Where they make a determination: (a) that the bringing of the section 7 proceedings or the making of the complaint is frivolous or

D vexatious; (b) that the section 7 proceedings have been brought, or the complaint made, out of time and that the time limit should not be extended; or (c) that the complainant does not have the right to bring the section 7 proceedings or make the complaint; the tribunal shall notify the complainant of that fact.

"(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the tribunal by rule 6(1).

E "(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the tribunal."

9 In Applications Nos IPT/01/62 and IPT/01/77 (unreported) 23 January 2003 the IPT held that rule 9(6) of the 2000 Rules, requiring the

F tribunal's proceedings to be conducted in private, was ultra vires section 69 of the 2000 Act as being incompatible with article 6 of the Convention which guarantees the right to a fair hearing before an independent and impartial tribunal; but "in all other respects the 2000 Rules are valid and binding on the tribunal and are compatible with articles 6, 8 and 10 of the Convention": para 12 of the decision.

G 10 Before passing to other statutory materials I should add that by force of paragraph 2 of Schedule 3 to the 2000 Act, the President of the IPT is required to be someone who holds or has held high judicial office. Other members must have held a relevant legal qualification for at least ten years. At the present time the President of the IPT is Mummery LJ and the Vice-President is Burton J.

11 I turn to the Human Rights Act 1998. Section 6(1) provides: "It is

H unlawful for a public authority to act in a way which is incompatible with a Convention right." Section 7 provides:

"*Proceedings*

"(1) A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal, or (b) rely on the Convention right or rights concerned in any legal proceedings, but only if he is (or would be) a victim of the unlawful act.

"(2) In subsection (1)(a) 'appropriate court or tribunal' means such court or tribunal as may be determined in accordance with rules; and proceedings against an authority include a counterclaim or similar proceeding.

"(3) If the proceedings are brought on an application for judicial review, the applicant is to be taken to have a sufficient interest in relation to the unlawful act only if he is, or would be, a victim of that act."

12 Lastly, CPR r 7.11:

"(1) A claim under section 7(1) of the 1998 Act in respect of a judicial act may be brought only in the High Court.

"(2) Any other claim under section 7(1)(a) of that Act may be brought in any court."

13 Sections 6 and 7 of the 1998 Act, CPR r 7.11, and sections 65(1)(2)(a)(b)(3)(a), 67(1) (as it relates to section 65(2)(a)(b)) and 70 of the 2000 Act, all came into force on 2 October 2000. Section 66 of the 2000 Act is to come into force on a day to be appointed. The 2000 Rules also came into force on 2 October 2000. Subordinate instruments are not ordinarily a legitimate aid to the construction of primary legislation; however to the extent that the 2000 Rules may be regarded as part and parcel of the same legislative scheme as is constituted by material provisions of the 1998 Act, the 2000 Act and the Civil Procedure Rules, I think we can consider what light they throw on the issue falling for decision.

The director's case

14 The director's case as it was advanced before Collins J is very straightforward. The claimant's claim pursuant to article 10 of the Convention is beyond doubt a claim within the meaning of section 7(1)(a) of the 1998 Act. It is therefore, by that provision, assigned exclusively to the "appropriate court or tribunal". Ordinarily, unless the claim is in respect of a judicial act, the "appropriate court or tribunal" is by force of CPR r 7.11 "any court". But where the claim (being within section 7(1)(a) of the 1998 Act) is brought "against any of the intelligence services" (section 65(3)(a) of the 2000 Act), the "appropriate court or tribunal" is by force of section 65(2)(a) of the 2000 Act, the IPT. This claim is brought against the Security Service, which is one of the intelligence services as defined by section 81 of the 2000 Act—the others are the Secret Intelligence Service and GCHQ. Accordingly the IPT is the "appropriate court or tribunal" and the High Court has no jurisdiction in the matter. Moreover it is not a question, so it is submitted, of the High Court's jurisdiction being ousted. The 1998 Act both created the Convention rights and by the same legislative act assigned their adjudication to the appropriate court or tribunal—in this case the IPT. The High Court never possessed any jurisdiction to be ousted. As I have said, the material provisions of the 1998 Act and the 2000 Act (and the CPR) all came into effect together, on 2 October 2000.

The claimant's original case

15 Mr Millar QC for the claimant seeks to advance a new point, not raised before Collins J, and I will come to that separately. The claimant's argument advanced before Collins J and accepted by him was and is to the following effect. Section 7(2) of the 1998 Act defines "the appropriate court or tribunal" as such court or tribunal as is determined by rules. On the face of it, by CPR r 7.11(2), the court or tribunal for the purposes of the claimant's article 10 claim is, simply, "any court", which manifestly includes the Administrative Court. As for section 65(2)(a) of the 2000 Act, it is submitted that it is highly significant that the opening words are "to be the only appropriate tribunal"—not "court or tribunal", which is the expression appearing in section 66(1) of the 2000 Act. This use of language shows that section 65(2)(a) of the 2000 Act does not touch the jurisdiction of any *court* properly so called. It merely assigns to the IPT a class of case which would otherwise have been heard by another *tribunal*.

16 Mr Millar submits that the effect of this proposition for the purpose of the present case is as follows. Specialist tribunals had been respectively established under the Security Service Act 1989 (which put the Security Service on a statutory footing) and the Intelligence Services Act 1994 (which put the Secret Intelligence Service and GCHQ on a statutory footing) in order to deal with complaints by persons aggrieved by anything they thought had been done by the relevant intelligence service in relation to them or their property. By section 70 of the 2000 Act the jurisdiction of those tribunals was abolished in relation to complaints arising after 2 October 2000. But the tribunals continue to exist and exercise jurisdiction in relation to complaints made before 2 October 2000. In light of this Mr Millar's argument is that the scope and purpose of section 65(2)(a) of the 2000 Act is to provide that claims which before 2 October 2000 would have been entertained in the earlier specialist tribunals must now, so far as they assert a violation of Convention rights, be brought before the IPT. But his client's article 10 claim has been properly brought as an autonomous action in the Administrative Court; that court is therefore the "appropriate court [or tribunal]" by force of CPR 7.11; section 65(2)(a) of the 2000 Act is not engaged.

The original case considered

17 In my judgment (leaving aside for the present Mr Millar's new point) the director's argument is correct, and the judge below was wrong to reject it.

18 First, section 65(2)(a) of the 2000 Act refers to "*any* proceedings under [section 7(1)(a)]" of the 1998 Act. (My emphasis.) The expression is unqualified. It plainly includes, on the face of it, proceedings such as these present proceedings. There is nothing to show that its scope is in some way limited by reference to the jurisdiction of the tribunals established under the 1989 and 1994 Acts or the jurisdiction of any other tribunals. The use in section 65(2)(a) of the 2000 Act of the term "tribunal" (in contrast to "court or tribunal" in section 66(1) of the 2000 Act) is in my view unsurprising and readily explained. The reference in section 66(1)(a)(b) of the 2000 Act is to a court or a tribunal, as it were as the case may be: the subject matter of the provision is a future order, as regards which the legislator cannot know

whether it will refer to a court or to a tribunal. By contrast section 65(2)(a) of the 2000 Act is enacted only in the context of the jurisdiction of the IPT already assigned by that subsection: and the IPT is, of course, a tribunal and not a court.

19 Secondly, the proposition that the scope of section 65(2)(a) of the 2000 Act is thus limited produces, in my view, wholly eccentric results. A complaint arising after 2 October 2000 which would, had it arisen before that date, have been dealt with by one of the earlier tribunals is now on the face of it assigned to the IPT by force of section 65(2)(b)(4) of the 2000 Act. "Complaint" is a term of art in section 65 of the 2000 Act, denoting a procedurally distinct form of claim. However the scope of such a complaint, which is given by section 65(4)(5) of the 2000 Act, is plainly wide enough to include an allegation "that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) of the 1998 Act": section 7(1) of the 1998 Act. Thus the effect of Mr Millar's argument is that if such a complaint indeed includes a claim to which section 7(1)(a) of the 1998 Act applies it is assigned to the IPT not under section 65(2)(b) of the 2000 Act, but under section 65(2)(a)—but by virtue only of the fact that it *is* a section 7(1)(a) claim under the 1998 Act. Yet any *other* section 7(1)(a) claim brought in court proceedings (such as the claimant's judicial review claim in this case), not being within section 65(2)(b)(4) of the 2000 Act, is by contrast not assigned to the IPT at all. So some section 7(1)(a) claims go to the IPT under section 65(2)(a) and others do not; yet the ones that do are in fact already there by force of section 65(2)(b).

20 There was some discussion in the course of argument as to the position relating to employment tribunals. Collins J referred to this [2008] 4 All ER 511, para 14:

> "the words used in section 65(2)(a) of the 2000 Act make sense if it is intended to exclude the jurisdiction of any other tribunal which might have jurisdiction in particular circumstances, for example, an employment tribunal."

It is clear that Crown servants whose work is or was in one of the intelligence services may bring proceedings in the employment tribunal. The Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004 (SI 2004/1861) contain special procedural provisions for the protection of national security where that falls for consideration: see Schedule 1, paragraph 54 and Schedule 2. But these circumstances, in my judgment, offer no material assistance to Mr Millar. If an employment claim against one of the intelligence services were to involve an allegation falling within section 7(1) of the 1998 Act, then, certainly, it would have to be brought in the IPT by force of section 65(2)(a) of the 2000 Act. But that of course is only because all claims against the intelligence services involving such an allegation must be brought in the IPT. I can see that, without the possibility of employment claims being diverted to the IPT by force of section 65(2)(a) of the 2000 Act, on Mr Millar's argument the *only* claims so diverted would be claims already assigned to the IPT by section 65(2)(b) of the 2000 Act—for the reasons I have given in para 19; and therefore the possibility of employment claims being so diverted at least gives some content to section 65(2)(a) of the 2000 Act beyond claims which are, in truth, already assigned to the IPT by section 65(2)(b) of the 2000 Act.

A That may soften the gross anomaly which Mr Millar's case produces; but it is a case that remains wholly eccentric.

21 As I have indicated in para 19, Mr Millar's argument is anomalous in two respects. (1) It effectively deprives section 65(2)(a) of the 2000 Act of independent content—subject to the possible inclusion of some employment claims. (2) It means that some, but not all, section 7(1)(a) claims under the 1998 Act against the intelligence services are assigned to the IPT: and B whereas there is logic in assigning all, or none, there is no logic whatever in assigning only some. That position is, I think, fortified by the content of the 2000 Rules. The provisions of rules 6, 9 and 13 which I have set out are apt to regulate any section 7(1)(a) proceedings under the 1998 Act against the intelligence services involving secure or sensitive information. Mr Millar's argument means that some such proceedings are covered by those C procedures and others are not. That cannot have been the legislative intention.

22 In the course of his submissions Mr Millar did not seek to make very great play of any suggestion that on the director's argument the High Court's jurisdiction is ousted by section 65(2)(a) of the 2000 Act—a possibility to which I referred in passing in describing the director's case. He was I think right not to do so. It is elementary that any attempt to oust altogether the D High Court's supervisory jurisdiction over public authorities is repugnant to the constitution. But statutory measures which confide the jurisdiction to a judicial body of like standing and authority to that of the High Court, but which operates subject to special procedures apt for the subject matter in hand, may well be constitutionally inoffensive. The IPT, whose membership I have described, offers with respect no cause for concern on this score. And E as I have noted the 2000 Rules have been held by the IPT to be Convention-compliant save for rule 9(6) which has accordingly fallen away.

23 Lastly on this part of the case, Mr Millar has placed much reliance on the decision of their Lordships' House in *R v Shayler* [2003] 1 AC 247. The House held in that case that a prosecution under the Official Secrets Act 1989 of a former member of the Security Service in respect of disclosures made by him in an unauthorised publication did not violate his article 10 F rights under the Convention, because he could have had recourse to judicial review to challenge any refusal of permission to publish (a recourse of which he had not sought to take advantage). There are indeed very clear references to the availability of judicial review, and its importance in context for the vindication of the Convention right, in their Lordships' opinions in *R v Shayler*. But the facts of the case happened in 1997 when the IPT did not G exist and the 2000 Act was not on the statute book. It is true that by the time the case went before their Lordships the new regime under the 2000 Act was in place; but no argument was addressed to their Lordships as to the possibility of any recourse to the IPT as opposed to judicial review at the hands of a person refused permission to publish. With great respect I do not consider, in those circumstances, that we may obtain any definitive guidance from *R v Shayler*.

H

The new point

24 With the court's permission granted at the hearing on 24 November 2008, Mr Millar raises a new point for the claimant. He submits that notwithstanding the fact that the director is named as defendant to the

claim, the proceedings are in substance brought against the Crown, and therefore are not "proceedings against any of the intelligence services" within the meaning of section 65(3)(a) of the 2000 Act. So section 65(2)(a) is not engaged, and the Administrative Court is and remains "the appropriate court or tribunal" for the purposes of section 7 of the 1998 Act.

25 Mr Millar submits that employees of the intelligence services are civil servants, who owe strict duties of confidence to the Crown. He referred to the current Civil Service Order in Council 1995; but the reference is misplaced, because that instrument applies to the Home Civil Service of which the Security Service is no part. However Mr Millar is right to submit that the general law now recognises that civil servants enter into legal relations with the Crown in the form of contracts of employment: *R v Lord Chancellor's Department, Ex p Nangle* [1991] ICR 743. In light of this it is said that the enhanced duty of confidence owed by members of the intelligence services is distinctly owed to the Crown, and so much is demonstrated by dicta in the "Spycatcher" litigation. Among other passages Mr Millar referred to the judgment at first instance of Scott J in *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 154, Donaldson MR, p 179, and Bingham LJ, p 213, in the Court of Appeal, and Lord Keith of Kinkel, p 256, in the House of Lords. Furthermore the relation between civil servants and the Crown is well exemplified, so it is submitted, by the document known as the Armstrong Memorandum (prepared by the then Secretary to the Cabinet, Sir Robert Armstrong, in 1985).

26 In consequence, submits Mr Millar, despite the form of these proceedings in which the director is named as defendant, the proceedings are in substance and in fact directed against the Crown as the claimant's former employer and the party to whom he owed and owes a duty of confidence. The proceedings are not, therefore, proceedings against any of the "intelligence services" within the meaning of section 65(3)(a) of the 2000 Act.

27 There is at once an obvious question: on this argument, what *is* the scope or content of the phrase "proceedings against any of the intelligence services" within section 65(3)(a) of the 2000 Act? The claimant's answer is that proceedings against the Security Service, for the purposes of section 65 of the 2000 Act, are *only* proceedings relating to the exercise of specific statutory functions assigned to the service; and the giving or withholding of consent to the publication of a previous employee's memoirs is not such a statutory function.

28 I cannot accept this submission. It proves too much. *All* the functions of the Security Service are, and have been since the coming into force of the Security Service Act 1989, statutory functions. Section 1 of the 1989 Act provides in part:

> "(2) The function of the service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
>
> "(3) It shall also be the function of the service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

A Section 2(2)(a) provides:

> "The Director-General shall be responsible for the efficiency of the service and it shall be his duty to ensure— (a) that there are arrangements for securing that no information is obtained by the service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of preventing or
B detecting serious crime . . ."

The giving or withholding of consent to a proposed publication written by a former member of the service is in my judgment incidental to these functions. Accordingly, the claimant's submission on this new argument leads to the conclusion that "proceedings against any of the intelligence services" in section 65(3)(a) of the 2000 Act—certainly so far as the phrase
C relates to the Security Service, and I can discern no distinction for this purpose between that service and the other intelligence services—is an empty category. But the statute cannot be construed so as to provide for such a result.

29 Mr Havers QC for the director accepts that the Security Service is an emanation of the Crown, having no legal personality of its own. It was not clothed in legal personality by the Security Service Act 1989. Its functions
D were merely thereby placed, as I have said, "on a statutory footing". All the intelligence services are emanations of the Crown. None has individual legal personality. It follows, as it seems to me, that the expression in section 65(3)(a) of the 2000 Act, "intelligence services", cannot be intended to refer to bodies having distinct legal personalities of their own, for in that case it would have no content at all. It can only be intended to refer to what
E are admittedly emanations of the Crown. Accordingly, the fact that the Crown is the legal personality standing as it were behind the Security Service does not take the Security Service out of section 65(3)(a) of the 2000 Act, nor therefore out of section 65(2)(a).

30 Mr Havers also pointed to documentation annexed to a witness statement produced by his instructing solicitor showing that the contractual arrangements into which the claimant entered with the Crown imposed
F obligations specifically owed to the Security Service, and made express provision for the procedures to be followed where a previous member of the service desires to publish a memoir. While these materials cannot affect the legal identity of the party with whom the claimant contracted—the Crown—they demonstrate, as Mr Havers submits, that the director is appropriately named as defendant in the proceedings.

G

Conclusion

31 For all these reasons I would allow the director's appeal, set aside the orders made by Collins J on 4 July 2008, and declare that the Administrative Court has no jurisdiction to entertain the claim under article 10 of the Convention. I should recall, however, that the claim includes other
H elements: accusations that the director's refusal of permission to publish was unreasonable and vitiated by bias. Mr Havers submits that the claimant should reformulate these aspects so as to constitute a complaint assigned to the IPT under section 65(2)(b) of the 2000 Act, so that the whole of the claimant's case will go before the IPT. If the claimant declines to take that course, Mr Havers submits that the Administrative Court should as a matter

of discretion refuse to entertain those parts of his case on the footing that he would not have exhausted prior remedies. That seems to me plainly to be right; but as at present advised I do not think we should pre-empt the Administrative Court's own decision on the matter.

RIX LJ

32 I am attracted by the pragmatic solution put forward by Dyson LJ which gives ultimately overriding effect to the absence of detailed rules of court to govern court proceedings which would have to deal with claims against the intelligence services. The purpose of such rules is to deal with the strong public interest in support of the protection of national security in the context of disputes concerning the intelligence services. The absence of detailed rules of court can be contrasted with the enactment of specialised rules for the purposes of cases not only before the Investigatory Powers Tribunal ("IPT") but also in employment tribunals: see the Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004. There is also force in the point, acknowledged by the judge and relied on by Dyson LJ, that the IPT is clearly the appropriate forum in which matters relating to surveillance and other like matters should be addressed: see para 57 below.

33 Nevertheless, I have been unable to persuade myself that the language of sections 65 and 66 of the 2000 Act permits this conclusion. We are called upon to interpret the phrase "the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998" found in section 65(2)(a) of the 2000 Act. The director submits that this amounts to an exclusion of the jurisdiction of the courts in relation to any proceedings under section 7(1)(a) of the 1998 Act. However, the phrase in question does not refer to the court(s) at all. It is common ground that there is another tribunal before which, but for section 65(2)(a) of the 2000 Act, a claim that a public authority (such as the intelligence services) has acted in a way made unlawful by section 6(1) of the 1998 Act might have been brought by way of proceedings under section 7 of the 1998 Act, and that is the employment tribunal. Therefore, section 65(2)(a) of the 2000 Act has content as referring to the IPT as "the only appropriate tribunal". If that phrase is intended to be an exclusion of the courts, then the exclusion is implicit rather than express.

34 Section 7(2) of the 1998 Act provides: "In subsection (1)(a) 'appropriate court or tribunal' means such court or tribunal as may be determined in accordance with rules." CPR r 7.11 provides that claims in respect of judicial acts must be brought in the High Court but: "Any other claim under section 7(1)(a) of that Act may be brought in any court." Thus, subject to the phrase in question in section 65(2)(a) of the 2000 Act, section 7 proceedings against a public authority may be brought in any court.

35 What light if any is thrown on the phrase "the only appropriate tribunal" by other parts of sections 65 and 66 of the 2000 Act? The following passages appear to me to be relevant:

(1) Section 65(2)(b) and section 65(4) of the 2000 Act each speaks of the IPT as "the appropriate forum" for complaints by a person aggrieved by conduct falling within section 65(5).

(2) Section 65(2)(d) says that the IPT has jurisdiction to hear and determine "any other such proceedings" (i e proceedings other than under

A section 7(1)(a) of the 1998 Act) falling within section 65(3) of the 2000 Act "as may be allocated to them in accordance with provision made by the Secretary of State by order". We have been told that no such order is as yet in force. Section 66(1) of the 2000 Act provides that any such order made under section 65(2)(d) of the 2000 Act "may provide for the tribunal to exercise jurisdiction in relation to that matter to the exclusion of the B jurisdiction of any court or tribunal", but that if it does so it must also confer a power on the IPT to remit the proceedings "to the court or tribunal which would have had jurisdiction apart from the order".

36 The following questions arise. Why, if the jurisdiction of the courts is excluded, does section 65(2)(a) of the 2000 Act speak of "the only appropriate tribunal" rather than of "the only appropriate forum" (to adopt the phraseology of section 65(2)(b) and section 65(4) of the 2000 Act)? Or C why does it not adopt the phraseology of section 66(1)(a) of the 2000 Act and speak in terms of "the exclusion of the jurisdiction of any court or tribunal"? Why does section 65(2)(b) and section 65(4) speak of the IPT as "the appropriate forum"?

37 There are no really satisfactory answers to any of these questions. It is true that section 7 of the 1998 Act speaks of "the appropriate court or D tribunal", which is language which no doubt section 65 of the 2000 Act is intended to reflect, and also true that the IPT is not a court, so that the language "the only appropriate court or tribunal" would be somewhat strange. However, strange or not, it would remain accurate, if it were intended to deny section 7 jurisdiction to any court or tribunal other than the IPT, to say that the jurisdiction of the IPT "shall be— (a) to be the only appropriate court or tribunal for the purposes of section 7 . . .". That would E have the virtue of tracking the language of section 7 precisely. If, however, it was felt to be unnatural to speak in terms of "court or tribunal", the word "forum" was at hand, in the phrase "appropriate forum", to bridge both courts and tribunals. Moreover, it would also have been possible to use the phraseology of section 66(1)(a) of the 2000 Act and make it plain that the section 7 jurisdiction of the IPT was "to the exclusion of the jurisdiction of F any court or tribunal".

38 It is said that the language of exclusiveness is not required since what was happening as of 2 October 2000 was an *allocation* of a new jurisdiction under the 1998 Act rather than any reallocation of an existing jurisdiction. However, I do not find the point very comforting. The fact is that CPR r 7.11 allocates section 7 proceedings in general to the courts and if an exception is to be carved out of that, even by primary legislation such as the G 2000 Act, one is entitled to think that such an exception would be achieved plainly and expressly, and not uncertainly and by means of implication.

39 Similarly, I would be more attracted (than I already am) by Dyson LJ's pragmatic solution with which I began if the effect of adopting it, and an imperative of adopting it, were to bring coherency to some overall scheme. However, I can find no such coherency in the provisions of the 2000 Act. As Dyson LJ has shown, there is a distinction made between H "proceedings" which are based on common law or statutory causes of actions (some of the latter of which can only be brought in tribunals such as employment tribunals) and "complaints". The only "proceedings" against the intelligence services which are allocated under section 65 of the 2000 Act are section 7 proceedings under the 1998 Act. All other proceedings are not

yet allocated (see section 65(2)(d) of the 2000 Act): if they were to be allocated, provision may or may not be made for the IPT to exercise jurisdiction to the exclusion of any court or tribunal. It would be understandable that proceedings *or* complaints which concerned subject matter of a particularly sensitive nature, such as surveillance, interception of communications, use of covert services and such like, should be assigned exclusively to the IPT, with its special rules, and removed entirely from all courts or other tribunals. That, however, is not the functional approach taken in section 65 of the 2000 Act. If one asks what is so special about section 7 proceedings under the 1998 Act against the intelligence services as to require them, of all proceedings, to be assigned solely to the IPT to the exclusion not only of any other tribunal (such as the employment tribunal) but of the courts as well, there is no ready answer. Certainly none has been suggested.

40 In sum, attracted as I am by a pragmatic solution, I have been unable to derive one from the words of the 2000 Act, or from any coherent purpose to be ascertained from its provisions. Therefore, albeit uneasily, I am forced back upon the judge's, admittedly somewhat unsatisfactory, palliative, namely that it may remain possible for the Administrative Court to refuse relief in its discretion in suitable cases, on the basis that there would be an alternative remedy before the IPT. I comfort myself, however, with the thought that in *R v Shayler* [2003] 1 AC 247, although the present point relating to the 2000 Act was not in issue, their Lordships saw no particular difficulty in suggesting judicial review as a suitable means by which a former member of the security intelligence services could challenge a refusal of permission to publish. Nor was that a mere matter of passing comment: it was the ground upon which their Lordships demonstrated that the would-be author had a remedy in the courts whereby he could seek a ruling by way of judicial review that the interference with his right of freedom of expression was greater than could be justified on grounds of national security.

41 I would therefore dismiss this appeal. I agree, however, that there is nothing in the "new point".

DYSON LJ

42 At first sight, there seems to be a good deal to be said in favour of the original case advanced by Mr Millar. First, the 2000 Act does not assign *all* claims against any of the intelligence services exclusively to the IPT (which is subject to the rules and special procedures which apply to that tribunal by virtue of the 2000 Rules). Even on the argument of Mr Havers, it is conceded that "complaints" falling within section 65(4) of the 2000 Act can be "reformulated" as legal rights of action against an intelligence service (whether statutory claims or common law claims) and these can be issued in a relevant tribunal or in the courts. An example of such a complaint is a claim against an intelligence service which can be brought before the employment tribunal. As Laws LJ has pointed out, the Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004 contain special provisions for the protection of national security in relation to such claims. It might, therefore, be said that, when enacting the 2000 Act, Parliament must be taken to have contemplated that a parallel jurisdiction would be enjoyed by the courts and tribunals other than the IPT and that special procedures would be established to deal with the national security

problems raised by claims against an intelligence service in such tribunals and the courts.

43 Secondly, there are points to be made on the language of the 2000 Act which, at first sight, might be said to lend support to the arguments of Mr Millar. The draftsman of section 65(2)(a) of the 2000 Act had the language of section 7(1)(a) of the 1998 Act in mind and was well aware of the difference between a court and a tribunal. Mr Millar emphasises the contrast between "the appropriate court or tribunal" (section 7(1)(a) of the 1998 Act) and "court or tribunal" (section 66(1)(a)(b) of the 2000 Act) on the one hand and "the only appropriate tribunal" (section 65(2)(a) of the 2000 Act) on the other hand. A further linguistic point that can be made is that the word "forum" is not used in section 65(2)(a) of the 2000 Act. This can be contrasted with section 65(2)(b) and 65(4) of the 2000 Act which provide that the IPT is "the appropriate forum" for any complaints falling within subsection (4). Since the generic word "forum" was present to the mind of the draftsman, it may be said that, if he had intended the IPT to have exclusive jurisdiction to entertain claims under section 7 of the 1998 Act, then he would have provided that the IPT was "the appropriate forum" in respect of such claims.

44 Despite these arguments, I agree with Laws LJ that the appeal should be allowed.

45 The judge was of the view that the director's construction required the jurisdiction of the court to be ousted. On well established principles, therefore, he identified [2008] 4 All ER 511, para 14 the relevant question as being whether section 65(2) "contains sufficiently clear and explicit words to require a construction that the courts' jurisdiction is ousted". He found in favour of the claimant principally because there are no such clear and explicit words in section 65.

46 I agree with Laws LJ that this is the wrong approach. The creation of Convention rights under the 1998 Act and the assignment of disputes about them to the appropriate court or tribunal were all part of the same legislative scheme which came into force on 2 October 2000. The courts did not previously have the jurisdiction to determine proceedings under the 1998 Act. No question of ouster of jurisdiction can therefore arise.

47 In my judgment, it is the fact that the relevant provisions of the 2000 Act, the 1998 Act and the 2000 Rules were all enacted and came into force at the same time as part of a single legislative scheme which points the way to the resolution of this appeal.

48 Rule 3 of the 2000 Rules provides that the 2000 Rules "apply to section 7 proceedings and to complaints". The 2000 Rules are detailed and elaborate. They are carefully drafted so as to achieve a balance between fairness to a complainant and the need to safeguard the relevant security interests. It seems to me to be inherently unlikely that Parliament intended to create an elaborate set of rules to govern proceedings against an intelligence service under section 7 of the 1998 Act in the IPT and yet contemplated that such proceedings might be brought before the courts without any rules. If it had been intended to allow a claimant to issue section 7 proceedings under the 1998 Act against an intelligence service in the courts, surely Parliament would have provided that the 2000 Rules (adapted as necessary) should apply to the court proceedings. Having enacted such detailed procedural rules in this difficult and sensitive area for proceedings before the IPT,

it would have been surprising if Parliament had intended to leave it to the courts to fashion their own rules. In this context, it is also not without significance that, as the Civil Procedure Rules demonstrate, Parliament routinely makes rules which govern court proceedings. They include rules which apply to proceedings in specialist courts.

49 In my judgment, the fact that the 2000 Rules apply to proceedings before the IPT and there are no corresponding rules in respect of section 7 proceedings under the 1998 Act against an intelligence service in the courts is a strong point in favour of the director's case. The question is whether the points identified at paras 42 and 43 above compel a different conclusion.

50 I do not consider that such a conclusion is required by the fact that the 2000 Rules govern "complaints" in respect of conduct falling within section 65(5) of the 2000 Act and the possibility exists that some such complaints can be "reformulated" as other statutory or common law claims and the 2000 Rules do not apply to those claims. The fact that such "complaints" can be so "reformulated" does not mean that they are the same as such other claims. A claim cannot be entertained by the courts unless it is in respect of a right of action recognised by the common law or a statute which gives the courts jurisdiction to entertain it. Similarly, a claim cannot be entertained by a tribunal unless it is one which the tribunal has jurisdiction to entertain. All this is trite enough. But it is important to keep in mind that a "complaint" is not the same thing as a claim in respect of a right of action which is recognised by the common law or a statute. A "complaint" is no more than a complaint by a person who is "aggrieved" by any conduct falling within section 65(5) which he believes satisfies the conditions stated in section 65(4) and (4A) as inserted by section 24(5) of the Identity Cards Act 2006. As regards the 2000 Act, it is irrelevant whether the complaint fortuitously can be reformulated as a claim in respect of a right of action recognised by the common law or a statute (other than the 2000 Act). The 2000 Act does not purport to touch such other claims against an intelligence service. In my view, there is no significance in the fact that such other claims can be brought in the courts and other tribunals to which the 2000 Rules do not apply.

51 On the other hand, a section 7 claim under the 1998 Act against an intelligence service is just that: a section 7 claim. It cannot be "reformulated" as a different kind of claim. It is explicitly dealt with by the 2000 Act.

52 As regards the linguistic points to which I refer above, I accept that the draftsman well understood the difference between a court and a tribunal. But in view of the fact that the IPT is a tribunal, it is not surprising that section 65(2)(a) of the 2000 Act provides that the IPT is the only tribunal before which section 7 proceedings may be brought. It would be odd to designate the IPT as "the only appropriate court or tribunal", because it is not a court. In the context of section 7(1) of the 1998 Act, a court is different from a tribunal.

53 I also accept that in section 65(2)(a) of the 2000 Act the draftsman could have referred to the IPT as "the appropriate forum" as he did in section 65(2)(b)(4) of the 2000 Act in relation to complaints. Had he done so, there would have been no scope for arguing that section 7 proceedings under the 1998 Act against an intelligence service could be brought before a court. It is not clear why the draftsman used the phrase "the appropriate forum" in section 65(2)(b)(4) of the 2000 Act. He could equally have used

A the phrase "the appropriate tribunal". I doubt whether he used the word "forum" to make it clear that "complaints" must be brought before the IPT and cannot be brought before the courts. That is because it goes without saying that complaints by persons aggrieved by any conduct falling within subsection (5) *cannot* be brought before the courts qua complaints. Courts do not have jurisdiction to entertain "complaints" as such. They have
B jurisdiction to determine claims which are based on rights of action which are recognised or established by the common law or statute. Other tribunals have jurisdiction to decide the matters in accordance with the statutes which govern their powers. Thus, although it is not clear why the phrase "appropriate forum" is used in section 65(2)(b) of the 2000 Act, I do not consider that the use of this phrase compels an interpretation of section 65(2)(a) which, for the reasons already given, is unlikely to have been
C intended by Parliament.

54 Mr Millar recognises the need to find content for his construction of section 65(2)(a) of the 2000 Act, ie to identify other tribunals which, but for section 65(2)(a), would have had jurisdiction to deal with section 7 proceedings under the 1998 Act against an intelligence service. He points to the tribunals established under the Security Service Act 1989 and the
D Intelligence Services Act 1994 as being tribunals having such jurisdiction. He submits that, although the jurisdiction of these tribunals was abolished by section 70 of the 2000 Act in relation to any complaint made after 2 October 2000, they continue to have jurisdiction in relation to complaints made before 2 October 2000. He submits that the words "the only appropriate tribunal" make it clear that the jurisdiction of the existing tribunals cannot be invoked in relation to complaints made after 2 October
E 2000 in respect of acts before that date.

55 But section 70(1) of the 2000 Act states that the provisions mentioned in subsection (2) "shall not apply in relation to any complaint made after [2 October 2000]". I doubt whether section 70 has anything to do with section 7 proceedings under the 1998 Act at all. The draftsman drew a clear distinction between a "complaint" (section 65(2)(b)(4) of the
F 2000 Act) and proceedings under section 7 of the 1998 Act: section 65(2)(a) of the 2000 Act. Section 70 of the 2000 Act relates to "any *complaint* made after the coming into force of this section" (emphasis added), ie not to section 7 proceedings under the 1998 Act. Moreover, I do not in any event see how section 7 proceedings could be brought before the tribunals established under the 1989 and 1994 Acts in respect of an act before 2 October 2000: section 7 of the 1998 Act did not come into force until that
G date. Further, the continuing existence and jurisdiction of these tribunals could not have been to enable them to deal with section 7 proceedings arising from complaints made after 2 October 2000 in respect of acts before that date. Section 70(1) of the 2000 Act explicitly states that the provisions set out in subsection (2) shall not apply to *any* complaint made after 2 October 2000, ie regardless of the date of the act of which complaint is
H made.

56 I do however accept that, although it was not the focus of Mr Millar's submissions, the employment tribunal is another tribunal which, but for section 65(2)(a) of the 2000 Act, would have had jurisdiction to deal with section 7 proceedings under the 1998 Act against an intelligence service.

57 There is a further reason why I prefer the director's construction. The judge acknowledged [2008] 4 All ER 511, para 26, that claims involving matters in relation to surveillance, interception of communications and the use of material obtained thereby, the use of covert services, and the acquisition of means whereby protected electronic data can be decrypted should be dealt with by the IPT. He said, at para 26, that it was

> "difficult to envisage circumstances in which such claims would properly be dealt with by the court since Parliament has clearly indicated that the [IPT] should deal with them."

He went on to say that nothing that he had said should encourage anyone who is concerned that his rights have been infringed by any such matters to seek redress through the court rather than the IPT. The circumstances of the present case, however,

> "are somewhat different and, although the [IPT] undoubtedly has jurisdiction, its procedures are less satisfactory and the issues are wider than those for which the 2000 Act specifically required it to be established."

He did not explain why its procedures are less satisfactory than those of the court. In considering whether the IPT is a satisfactory tribunal to determine issues that are wider than those for which the 2000 Act required it to be established, the composition of the tribunal should not be overlooked: see para 10 of Laws LJ's judgment.

58 The judge said that a section 7 claim under the 1998 Act which, by reason of its subject matter and the issues raised, is not suited for determination by the court could be dismissed or stayed on that ground. It may be that the Administrative Court could, in the exercise of its discretion, refuse relief in such a case. But it is by no means certain that the same can be said of the county court. In any event, such a solution would introduce undesirable uncertainty and satellite litigation. I do not believe that this can have been intended by Parliament.

59 For these reasons, I would allow this appeal. I should add that I agree with what Laws LJ has said about the "new point" and have nothing to add.

Appeal allowed.
Permission to appeal refused.

8 May 2009. The Appeal Committee of the House of Lords (Lord Phillips of Worth Matravers, Lord Walker of Gestingthorpe and Baroness Hale of Richmond) allowed a petition by the claimant for leave to appeal.

BJU

APPEAL

The claimant appealed.

JUSTICE was given permission to intervene on the appeal. On 1 October 2009 the proceedings were transferred to and continued in the Supreme Court of the United Kingdom pursuant to section 57 of and paragraph 3(1) of Schedule 10 to the Constitutional Reform Act 2005.

The facts are stated in the judgment of Lord Brown of Eaton-under-Heywood JSC.

A *Gavin Millar* QC and *Guy Vassall-Adams* (instructed by *Bindmans LLP*) for the claimant.

The natural meaning of the word "tribunal" in section 65(2)(a) of the Regulation of Investigatory Powers Act 2000 is not "court or tribunal". In statutes dealing with the jurisdiction of courts and tribunals a "tribunal" is a body with judicial functions but is specially constituted, invariably by
B statute. It may consist of a judge or a court but it lacks the normal general jurisdiction of a court. A "tribunal" is therefore distinct from a "court", which means a court with a general jurisdiction.

Read in context the "tribunal" in section 65(2)(a) cannot have an extended meaning as contended for by the director. Section 65(2) is cross-referring to section 7(2) of the Human Rights Act 1998. In section 7(2) an appropriate court is different from an appropriate tribunal. The same
C should be true when the concept of an appropriate tribunal in the 1998 Act is incorporated by reference in the 2000 Act. The word "only" should not be read so as to give the words "appropriate tribunal" a meaning which would oust the jurisdiction of the courts in relation to this particular type of proceedings. If that had been Parliament's intention it would surely have said so in certain terms rather than in such an obscure manner.

D The fact that the Investigatory Powers Tribunal ("IPT") does not have to give reasons for its decision is a disadvantage. The claimant has no way of seeing the case he has to meet and there is no possibility of judicial review. The court must lean against the construction of a statute which would lead to a violation of the right to a fair trial The word "only" should be strictly construed in favour of the claimant and section 65(2) must be read in a way which gives the claimant a right to take a case concerned with his right to
E freedom of expression under article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms to the courts.

Construing section 65(2)(a) in a way which denies the claimant access to the courts would force him to assert his right to freedom of expression under article 10 of the Convention in a tribunal which does not meet the standards required under article 6(1). The procedures of the IPT do not meet those
F standards in several ways: the restrictions on the disclosure of information; the absence of a public hearing; the inability of a complainant to call and cross-examine witnesses; the restrictions on the notification of IPT decisions; and the absence of any right of appeal. A construction which allows the claimant access to the High Court in judicial review proceedings does not have any adverse consequences for the state.

The principle of legality requires that fundamental rights cannot be
G overriden by general or ambiguous words. Where there is a justiciable issue access to the courts should not be denied save by clear words. The court must presume, in the absence of a clear contrary intention, that Parliament did not intend to create inconsistency in the law relating to jurisdiction over proceedings under section 7(1)(a) of the 1998 Act.

Section 65(2)(a) must be read in a way which is compatible with the
H claimant's right to a fair trial of his claim under section 7(1)(a) of the Human Rights Act 1998 against the Security Service. It must therefore be read in a way which allows him to bring his claim in the High Court, and it is possible to read the section in that way. [Reference was made to *R v Shayler* [2003] 1 AC 247; *Jersild v Denmark* (1994) 19 EHRR 1 and *Ghaidan v Godin-Mendoza* [2004] 2 AC 557.]

Lord Pannick QC and *Tom Hickman* (instructed by *Freshfields Bruckhaus Deringer LLP*) for the intervener. A

The submissions made by the claimant are supported. Section 65(2) of the 2000 Act should be construed so as to give those bringing claims the right to go to a tribunal other than the IPT. The procedures of the IPT are impossible to reconcile with article 6(1) of the Convention. It has no adversarial process and a claimant has no right to see the evidence or documents or to know the identity of witnesses unless the security services consent. It gives power to the security services to decide what should be disclosed and gives no power to the IPT. B

The IPT publishes no judgment as to what it has decided and as to the merits of the case. Parliament cannot have intended that a claimant must use a tribunal which breaches basic human rights.

C

Jonathan Crow QC and *Jason Coppel* (instructed by *Treasury Solicitor*) for the director.

The natural meaning of the word "tribunal" in section 65 of the 2000 Act encompasses both courts and tribunals and is therefore capable of referring to the courts. Parliament's consistent practice in legislation designating a particular court or tribunal as the relevant forum for particular proceedings has been to adopt that natural meaning and to use the term "tribunal" to D encompass not only statutory and even non-statutory tribunals, but ordinary courts as well. The word "only" in section 65(2)(a) must be given force and it is deliberately introduced and meant to denote exclusivity. The word "any" in section 65(2)(a) is also important. The combination of those two words show that the IPT was meant to be the exclusive tribunal for any proceedings under section 65(2)(a).

E

Parliament intended simply that the IPT should be the only judicial body with jurisdiction over proceedings in the relevant categories brought under section 7(1)(a) of the Human Rights Act 1998. That use of the term "tribunal" is consistent with the requirement under the Human Rights Convention that civil rights be determined by an independent and impartial tribunal established by law. The long title of the 2000 Act shows that the functions of the IPT are not confined to investigatory matters. The dispute F over the claimant's manuscript falls within the scope of the long title and the heading of Part IV of the Act. The IPT was intended to deal with precisely the article 10 allegations made by the claimant.

The Court of Appeal correctly interpreted section 65(2)(a) of the 2000 Act. Its approach is supported by other related pieces of legislation where the word "tribunal" is used: section 195(1) of the Extradition Act G 2003, section 11 of the Prevention of Terrorism Act 2005.

The procedural regime governing the IPT procedure is specifically designed to enable the intelligence services to participate in hearings against them in a way that they cannot do before the ordinary courts. The primary legislation contemplates a regime intended to achieve the purpose in section 69 of the 2000 Act and to achieve a penetrating scrutiny to protect the public interest. Specific to the IPT is the power to obtain information H and the unqualified power to demand information from officers of the Crown. The intelligence services are able to present sensitive information to the IPT without any of the constraints which would be felt in litigation in the ordinary courts. The IPT Rules provide stringent protections for the secrecy

A and security of sensitive intelligence material and the preservation of the "neither confirm nor deny" policy.

The admissibility of evidence in the IPT is wholly different from any ordinary court and the normal rules of evidence do not apply. The IPT is empowered to scrutinise closely all relevant evidence. Nothing is inadmissible and nothing may be excluded or withheld. Public interest immunity is not a bar to admitting evidence before the IPT. As a result the B IPT is able to provide full, effective scrutiny of sensitive intelligence material in a manner which is not possible or appropriate in the ordinary courts.

The decision in *R v Shayler* [2003] 1 AC 247 is not of help on the issue of construction in this case because the interpretation or scope of section 65 of the 2000 Act was not before the House of Lords in that case.

C The Court of Appeal's interpretation of section 65(2)(a) of the 2000 Act does not involve any general ouster of the court's jurisdiction. The section does not oust the supervisory jurisdiction of the High Court or limit or deny access to the courts. It is concerned only with a specific statutory cause of action against a public authority under section 7(1)(a) of the Human Rights Act 1998. It can be contrasted with the position in *Pyx Granite Co Ltd v Ministry of Housing and Local Government* [1960] AC 260.

D This case is also different from *Anisminic Ltd v Foreign Compensation Commission* [1969] 2 AC 147. There is no prevention of scrutiny by the ordinary courts in section 65(2)(a). What is being done in that section is an allocation of remedial routes. The public law jurisdiction of the administrative courts is not being ousted because the IPT does not deal with an administrative jurisdiction. The Administrative Court has a discretion to E consider whether, as a matter of form and substance, the claim was a human rights claim.

There is no breach of article 6(1) of the Convention. The demands of article 6 are not constant in all cases and the European Court of Human Rights has recognised that the protection of national security is a legitimate aim which may entail modification of or limitations on the ordinary F requirements of article 6(1). The demands of national security can justify restrictions being placed on normal court proceedings.

The security services are an essential part of the state's obligation under the Human Rights Act 1998 to protect its citizens. States have a wide margin of appreciation as to the means by which they achieve the legitimate aims such as safeguarding national security provided there are adequate safeguards against abuse of the protected rights. The margin of G appreciation is wider in relation to civil proceedings than to criminal proceedings.

The European Commission of Human Rights specifically considered and rejected complaints regarding the procedures of the predecessor to the IPT and endorsed those procedures: see *Esbester v United Kingdom* (1993) 18 EHRR CD 72. That decision has been affirmed in subsequent cases. The rules and procedures of the IPT go much further towards ensuring H procedural protection for complainants than did those of its predecessors. Therefore on current Strasbourg authority there is no incompatibility between the rules and procedures of the IPT and article 6(1) of the Convention. The Supreme Court should not go further than Strasbourg authority goes in relation to the procedures of the IPT.

There is nothing in the restrictions on disclosure of information in rule 6 of the IPT Rules which is incompatible with article 6(1) of the Convention. There is no absolute bar on disclosure by the IPT of information or documents provided to it, or the identity of any witness. There is no blanket provision for secrecy. The specific restriction on disclosure does not apply where consent has been given by the person specified in rule 6(3) and provided that disclosure would not be contrary to interests specified in rule 6(1).

The IPT has power to hold inter partes oral hearings in public in appropriate cases and it is open to the claimant to seek to persuade the IPT that a public hearing would be appropriate in this case. However there is no breach of article 6(1) where the IPT decides not to hold a public hearing. Article 6(1) expressly provides that hearings may be held in private in the interests of national security in a democratic society.

Article 6(1) does not import any absolute right to call or cross-examine witnesses. As to the absence of the public pronouncement of a fully reasoned judgment by the IPT, the claimant has already been given a clear and detailed statement of the director's objections to each of the disputed passages in the manuscript. To the extent that the IPT upholds the director's refusal of permission in relation to those particular passages, the claimant will be in a good position to understand why the refusal has been upheld. Article 6(1) does not guarantee any right of appeal.

Millar QC replied.

The court took time for consideration.

9 December 2009. **LORD BROWN OF EATON-UNDER HEYWOOD** JSC, with whom all members of the court agreed.

1 A is a former senior member of the Security Service, B its Director of Establishments. A wants to publish a book about his work in the Security Service. For this he needs B's consent: unsurprisingly, A is bound by strict contractual obligations as well as duties of confidentiality and statutory obligations under the Official Secrets Act 1989. On 14 August 2007, after lengthy top secret correspondence (and following final consideration by the Director General), B refused to authorise publication of parts of the manuscript. The correspondence (and annexures) described in detail the Security Services's national security objections to disclosure. On 13 November 2007 A commenced judicial review proceedings to challenge B's decision. He claims that it was unreasonable, vitiated by bias and contrary to article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the right to freedom of expression. Is such a challenge, however, one that A can bring in the courts or can it be brought only in the Investigatory Powers Tribunal ("the IPT")? That is the issue now before the court and it is one which depends principally upon the true construction of section 65(2)(a) of the Regulation of Investigatory Powers Act 2000 ("RIPA"):

> "The jurisdiction of the tribunal shall be— (a) to be the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 in relation to any proceedings under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights) which fall within subsection (3) of this section . . ."

A Subsection (3) provides that proceedings fall within this section if— "(a) they are proceedings against any of the intelligence services . . ."

2 Collins J [2008] 4 All ER 511 decided that the Administrative Court had jurisdiction to hear A's challenge (4 July 2008). The Court of Appeal (Laws and Dyson LJJ, Rix LJ dissenting), ante, p 5, reversed that decision, holding that exclusive jurisdiction lies with the IPT (18 February 2009).

B 3 Before turning to the rival contentions it is convenient to set out the legislative provisions most central to the arguments advanced. The Human Rights Act 1998 ("HRA") by section 7 provides:

> "(1) A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may— (a) bring proceedings against the authority under this Act in the
C appropriate court or tribunal, or (b) rely on the Convention right or rights concerned in any legal proceedings, but only if he is (or would be) a victim of the unlawful act.
>
> "(2) In subsection (1)(a) 'appropriate court or tribunal' means such court or tribunal as may be determined in accordance with rules; and proceedings against an authority include a counterclaim or similar proceeding . . .
D "(9) In this section 'rules' means— (a) in relation to proceedings before a court or tribunal outside Scotland, rules made by . . . the Lord Chancellor or the Secretary of State for the purposes of this section or rules of court . . ."

Pursuant to section 7(9), CPR r 7.11 (introduced, like HRA, with effect from 2 October 2000) provides:

E
> "(1) A claim under section 7(1)(a) of the Human Rights Act 1998 in respect of a judicial act may be brought only in the High Court.
>
> "(2) Any other claim under section 7(1)(a) of that Act may be brought in any court."

4 The only tribunals upon whom section 7(1)(a) HRA jurisdiction has
F been conferred by rules made under section 7(9) are the Special Immigration Appeals Commission ("SIAC") and the Proscribed Organisations Appeal Commission ("POAC")—not, contrary to the Court of Appeal's understanding (see paras 20, 33 and 56 of the judgments below), the employment tribunal.

5 I have already set out section 65(2)(a) of RIPA. Section 65(1) made provision for the establishment of the IPT and Schedule 3 to the Act
G provides for its membership. Currently its President is Mummery LJ and its Vice-President, Burton J. Section 67(2) provides:

> "Where the tribunal hear any proceedings by virtue of section 65(2)(a), they shall apply the same principles for making their determination in those proceedings as would be applied by a court on an application for
H judicial review."

Section 67(7) empowers the tribunal "to make any such award of compensation or other order as they think fit". Section 67(8) provides:

> "Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the

tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court."

Section 68(1) provides: "Subject to any rules made under section 69, the tribunal shall be entitled to determine their own procedure in relation to any proceedings, complaint or reference brought before or made to them." Section 68(4) provides:

"Where the tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of section 69(2)(i)) shall be confined, as the case may be, to either— (a) a statement that they have made a determination in his favour; or (b) a statement that no determination has been made in his favour."

6 Section 69 confers on the Secretary of State the rule-making power pursuant to which were made the Investigatory Powers Tribunal Rules 2000 (SI 2000/2665) ("the Rules"). Section 69(6) provides:

"In making rules under this section the Secretary of State shall have regard, in particular, to— (a) the need to secure that matters which are the subject of proceedings, complaints or references brought before or made to the tribunal are properly heard and considered; and (b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic wellbeing of the United Kingdom or the continued discharge of the functions of any of the intelligence services."

7 Rule 13(2) provides that where the tribunal make a determination in favour of the complainant they shall provide him with a summary of that determination including any findings of fact (to this extent qualifying section 68(4)(a) of the Act). Rule 6(1) gives effect to section 69(6)(b) by providing that the tribunal shall carry out their functions in such a way as to meet the stipulated need with regard to the non-disclosure of information. The effect of rule 6(2)(3) is that, save with the consent of those concerned, the tribunal may not disclose to the complainant or any other person any information or document disclosed or provided to them in the course of any hearing or the identity of any witness at that hearing. Rule 9 provides that the tribunal are under no duty to hold oral hearings and may hold separate oral hearings for the complainant and the public authority against which the proceedings are brought. Rule 9(6) provides that: "The tribunal's proceedings, including any oral hearings, shall be conducted in private."

8 In *Applications Nos IPT/01/62* and *IPT/01/77* (23 January 2003) the IPT ruled on various preliminary issues of law regarding the legality of a number of the rules. They held that rule 9(6) was ultra vires section 69 of RIPA as being incompatible with article 6 of the Convention but that "in all other respects the Rules are valid and binding on the tribunal and are compatible with articles 6, 8 and 10 of the Convention" (para 12 of the IPT's 83-page ruling which is itself the subject of a pending application before the European Court of Human Rights ("ECtHR")). Consequent on their ruling on rule 9(6) the IPT published the transcript of the hearing in that case and now hear argument on points of law in open court.

A 9 A accepts that the legal challenge he is making to B's decision is properly to be characterised as proceedings under section 7(1)(a) of HRA within the meaning of section 65(2)(a) of RIPA (and not, as he had argued before the judge at first instance, that he should be regarded merely as relying on his article 10 rights pursuant to section 7(1)(b) HRA), and that these are proceedings against one of the Intelligence Services within the B meaning of section 65(3)(a) (and not, as he had argued before the Court of Appeal, against the Crown). He nevertheless submits that he is not required by section 65(2)(a) to proceed before the IPT. His first and main argument—the argument which prevailed before Collins J and was accepted also by Rix LJ—is that he is entitled to proceed *either* by way of judicial review *or* before the IPT, entirely at his own choice. Section 65(2)(a), he submits, excludes the section 7(1)(a) jurisdiction of any other tribunal but C not that of the courts. His second and alternative argument (not advanced in either court below) is that, even if section 65(2)(a) is to be construed as conferring exclusive section 7(1)(a) jurisdiction on the IPT, it does so only in respect of proceedings against the intelligence services arising out of the exercise of one of the investigatory powers regulated by RIPA. This, of course, would involve narrowing the apparent width of the expression D "proceedings against any of the intelligence services" in section 65(3)(a) and, if correct, means that A here could not proceed before the IPT even if he wished to do so.

10 JUSTICE have intervened in the appeal in support of A's submissions. Like A, they urge us to adopt as narrow a construction of section 65 as possible, first, so as not to exclude the jurisdiction of the ordinary courts and, secondly, to avoid a construction which they submit E will inevitably give rise to breaches of other Convention rights, most notably the article 6 right to a fair hearing.

Argument 1—section 65(2)(a) excludes only the jurisdiction of other tribunals

11 This argument focuses principally upon the use of the word F "tribunal" in the expression "only appropriate tribunal" in section 65(2)(a). A says it that it means tribunals only and not courts; B says that it encompasses both. A says that if it was intended to exclude courts as well as tribunals it would have used the same expression, "the appropriate forum", as was used in section 65(2)(b), 65(4) and 65(4A) of RIPA (as amended by section 24(5) of the Identity Cards Act 2006). B points out that those three G provisions all deal with "complaints", for which provision had originally been made in the Security Service Act 1989 and the Intelligence Services Act 1994 and which are not the same as legal claims, "forum" being, therefore, a more appropriate term to describe the venue for their resolution.

12 Plainly the word "tribunal", depending on the context, can apply either to tribunals in contradistinction to courts or to both tribunals and courts. As B points out, section 195(1) of the Extradition Act 2003 describes H "the appropriate judge" (a designated district judge) as "the only appropriate tribunal" in relation to section 7(1)(a) HRA proceedings. So too section 11 of the Prevention of Terrorism Act 2005 describes "the court" (as thereafter defined) as "the appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998".

13 Section 7(2) of HRA itself appears to require that a court *or* tribunal is designated as *the* "appropriate court or tribunal", not that *both* are designated. Couple with that the use of the word "only" before the phrase "appropriate tribunal" in section 65 and it seems to me distinctly unlikely that Parliament was intending to leave it to the complainant to choose for himself whether to bring his proceedings in court or before the IPT.

14 There are, moreover, powerful other pointers in the same direction. Principal amongst these is the self-evident need to safeguard the secrecy and security of sensitive intelligence material, not least with regard to the working of the intelligence services. It is to this end, and to protect the "neither confirm nor deny" policy (equally obviously essential to the effective working of the services), that the Rules are as restrictive as they are regarding the closed nature of the IPT's hearings and the limited disclosure of information to the complainant (both before and after the IPT's determination). There are, however, a number of counterbalancing provisions both in RIPA and the Rules to ensure that proceedings before the IPT are (in the words of section 69(6)(a)) "properly heard and considered". Section 68(6) imposes on all who hold office under the Crown and many others too the widest possible duties to provide information and documents to the IPT as they may require. Public interest immunity could never be invoked against such a requirement. So too sections 57(3) and 59(3) impose respectively upon the Interception of Communications Commissioner and the Intelligence Services Commissioner duties to give the IPT "all such assistance" as it may require. Section 18(1)(c) disapplies the otherwise highly restrictive effect of section 17 (regarding the existence and use of intercept material) in the case of IPT proceedings. And rule 11(1) allows the IPT to "receive evidence in any form, and [to] receive evidence that would not be admissible in a court of law". All these provisions in their various ways are designed to ensure that, even in the most sensitive of intelligence cases, disputes can be properly determined. None of them are available in the courts. This was the point that so strongly attracted Dyson LJ in favour of *B's* case in the court below. As he pithily put it, ante, p 19, para 48:

> "It seems to me to be inherently unlikely that Parliament intended to create an elaborate set of rules to govern proceedings against an intelligence service under section 7 of the 1998 Act in the IPT and yet contemplated that such proceedings might be brought before the courts without any rules."

15 A further telling consideration against the contention that section 65(2)(a) is intended only to exclude other tribunals with jurisdiction to consider section 7(1)(a) HRA claims is that there are in fact none such with section 7(1)(a) jurisdiction over the categories of claim listed in section 65(3). As stated, at para 4 above, only SIAC and POAC have section 7(1)(a) jurisdiction and in each instance that is with regard to matters outside the scope of section 65. The Court of Appeal were under the misapprehension that the employment tribunal too had section 7(1)(a) jurisdiction and were accordingly mistaken in supposing, as Rix LJ put it, ante, p 16, para 33, that "Therefore, section 65(2)(a) of the 2000 Act has content as referring to the IPT as 'the only appropriate tribunal' ".

16 In the light of these various considerations it is hardly surprising that A himself recognises that this construction produces "a slightly

A unsatisfactory legislative outcome", although he submits that "this is a small price to pay for protecting the article 6 rights of claimants and respecting the principle that access to the courts should not be denied save by clear words", a submission to which I shall come after considering A's alternative contended-for construction.

B *Argument 2—section 65(2)(a) confers exclusive jurisdiction on the IPT but only in respect of proceedings arising out of the exercise of one of the RIPA regulated investigatory powers*

17 Although this was not an argument advanced at any stage below, I confess to having been attracted to it for a while. After all, in enacting RIPA, Parliament must have had principally in mind the use and abuse of the particular investigatory powers regulated by the Act and there would not C appear to be the same need for secrecy, the withholding of information and the "neither confirm nor deny" policy in the case of an ex-officer as in the case of someone outside the intelligence community.

18 The difficulties of such a construction, however, are obvious and in the end, to my mind, insurmountable. As already observed, it would involve reading into section 65(3)(a) limiting words which are simply not there. D This would be difficult enough at the best of times. Given, however, that other paragraphs of section 65(3) are in fact more obviously directed to complaints of abuse of the intelligence services' regulatory powers (see particularly section 65(3)(d) read with sections 65(5)(a) and 65(7), none of which I have thought it necessary to set out), it seems to me quite impossible to construe the section as this argument invites us to do.

19 Nor, indeed, on reflection, does it seem right to regard proceedings E of the kind intended here as immune from much the same requirement for non-disclosure of information as other proceedings against the intelligence services. As B points out, it is perfectly possible that the security service will ask the tribunal hearing this dispute to consider additional material of which A may be unaware (and of which the security service is properly concerned that he should remain unaware) which leads it to believe that the publication F of A's manuscript would be harmful to national security. On any view, moreover, the proceedings by which any tribunal comes to determine whether the disputed parts of the manuscript can safely be published would have to be heard in secret. Again, therefore, the existence of the IPT Rules designed to provide for just such proceedings and the lack of any equivalent rules available to the courts points strongly against this alternative G construction also.

20 Are there, however, sufficiently strong arguments available to A (and JUSTICE) to compel the court, with or without resort to section 3 of HRA, to adopt a contrary construction of section 65? It is convenient to consider these arguments under three broad heads.

(i) Ouster

H 21 A and JUSTICE argue that to construe section 65 as conferring exclusive jurisdiction on the IPT constitutes an ouster of the ordinary jurisdiction of the courts and is constitutionally objectionable on that ground. They pray in aid two decisions of high authority: *Pyx Granite Co Ltd v Ministry of Housing and Local Government* [1960] AC 260 and

Anisminic Ltd v Foreign Compensation Commission [1969] 2 AC 147. To my mind, however, the argument is unsustainable. In the first place, it is evident, as the majority of the Court of Appeal pointed out, that the relevant provisions of RIPA, HRA and the CPR all came into force at the same time as part of a single legislative scheme. With effect from 2 October 2000 section 7(1)(a) HRA jurisdiction came into existence (i) in respect of section 65(3) proceedings in the IPT pursuant to section 65(2)(a), and (ii) in respect of any other section 7(1)(a) HRA proceedings in the courts pursuant to section 7(9) and CPR r 7.11. True it is, as Rix LJ observed, that CPR r 7.11(2) does not explicitly recognise the exception to its apparent width represented by section 65(2)(a). But that is not to say that section 65(2)(a) ousts some pre-existing right.

22 This case, in short, falls within the principle recognised by the House of Lords in *Barraclough v Brown* [1897] AC 615—where, as Lord Watson said, at p 622: "The right and the remedy are given uno flatu, and the one cannot be dissociated from the other"—rather than the principle for which *Pyx Granite* stands, at p 286: "It is a principle not by any means to be whittled down that the subject's recourse to Her Majesty's courts for the determination of his rights is not to be excluded except by clear words." Distinguishing *Barraclough v Brown*, Viscount Simonds pointed out that the statute there in question could be construed as merely providing an alternative means of determining whether or not the company had a pre-existing common law right to develop their land; it did not take away "the inalienable remedy . . . to seek redress in [the courts]". Before 2 October 2000 there was, of course, no pre-existing common law or statutory right to bring a claim based on an asserted breach of the Convention. Section 65(2)(a) takes away no "inalienable remedy".

23 Nor does *Anisminic* assist A. The ouster clause there under consideration purported to remove any judicial supervision of a determination by an inferior tribunal as to its own jurisdiction. Section 65(2)(a) does no such thing. Parliament has not ousted judicial scrutiny of the acts of the intelligence services; it has simply allocated that scrutiny (as to section 7(1)(a) HRA proceedings) to the IPT. Furthermore, as Laws LJ observed, ante, p 13, para 22:

> "statutory measures which confide the jurisdiction to a judicial body of like standing and authority to that of the High Court, but which operates subject to special procedures apt for the subject matter in hand, may well be constitutionally inoffensive. The IPT . . . offers . . . no cause for concern on this score."

True it is that section 67(8) of RIPA constitutes an ouster (and, indeed, unlike that in *Anisminic*, an unambiguous ouster) of any jurisdiction of the courts over the IPT. But that is not the provision in question here and in any event, as A recognises, there is no constitutional (or article 6) requirement for any right of appeal from an appropriate tribunal.

24 The position here is analogous to that in *Farley v Secretary of State for Work and Pensions (No 2)* [2006] 1 WLR 1817 where the statutory provision in question provided that, on an application by the Secretary of State for a liability order in respect of a person liable to pay child support, "the court . . . shall not question the maintenance assesment under which the payments of child support maintenance fall to be made". Lord Nicholls

of Birkenhead, with whom the other members of the committee agreed, observed, at para 18:

> "The need for a strict approach to the interpretation of an ouster provision . . . was famously confirmed in the leading case of *Anisminic* . . . This strict approach, however, is not appropriate if an effective means of challenging the validity of a maintenance assessment is provided elsewhere. Then section 33(4) is not an ouster provision. Rather, it is part of a statutory scheme which allocates jurisdiction to determine the validity of an assessment and decide whether the defendant is a 'liable person' to a court other than the magistrates' court."

(ii) Convention rights

25 A and JUSTICE submit that to force this article 10 challenge into the IPT would inevitably result in breaches of article 6. In support of this submission they rely principally upon the following features of the IPT's procedures: first, that the entire hearing (save for purely legal argument) will be not only private but secret, indeed claimants may not even be told whether a hearing has been or will be held; secondly, that the submissions and evidence relied on respectively by the claimant and the respondent may be considered at separate hearings; thirdly, that only with the respondent's consent will the claimant be informed of the opposing case or given access to any of the respondent's evidence; fourthly, that no reasons will be given for any adverse determination. All of this, runs the argument, is flatly contrary to the basic principles of open justice: that there should be a public hearing at which the parties have a proper opportunity to challenge the opposing case and after which they will learn the reasons for an adverse determination.

26 As, however, already explained, at para 14, claims against the intelligence services inevitably raise special problems and simply cannot be dealt with in the same way as other claims. This, indeed, has long since been recognised both domestically and in Strasbourg. It is sufficient for present purposes to cite a single paragraph from the speech of Lord Bingham of Cornhill in *R v Shayler* [2003] 1 AC 247, para 26 (another case raising article 10 considerations):

> "The need to preserve the secrecy of information relating to intelligence and military operations in order to counter terrorism, criminal activity, hostile activity and subversion has been recognised by the European Commission and the court in relation to complaints made under article 10 and other articles under the Convention: see *Engel v The Netherlands (No 1)* (1976) 1 EHRR 647, paras 100–103; *Klass v Federal Republic of Germany* (1978) 2 EHRR 214, para 48; *Leander v Sweden* (1987) 9 EHRR 433, para 59; *Hadjianastassiou v Greece* (1992) 16 EHRR 219, paras 45–47; *Esbester v United Kingdom* (1993) 18 EHRR CD 72, 74; *Brind v United Kingdom* (1994) 18 EHRR CD 76, 83–84; *Murray v United Kingdom* (1994) 19 EHRR 193, para 58; *Vereniging Weekblad Bluf! v The Netherlands* (1995) 20 EHRR 189, paras 35, 40. The thrust of these decisions and judgments has not been to discount or disparage the need for strict and enforceable rules but to insist on adequate safeguards to ensure that the restriction does not exceed what is necessary to achieve the end in question. The acid test is whether,

in all the circumstances, the interference with the individual's Convention right prescribed by national law is greater than is required to meet the legitimate object which the state seeks to achieve. The OSA 1989, as it applies to the appellant, must be considered in that context."

27 In one of the Strasbourg cases there referred to, *Esbester v United Kingdom* (1993) 18 EHRR CD 72, and indeed in a series of other cases brought against the UK at about the same time, the Strasbourg commission rejected complaints as to the form of proceedings adopted by the Security Service Tribunal and the Interception of Communications Tribunal, not least as to the absence of a reasoned determination.

28 I acknowledge that later in his opinion in *R v Shayler* [2003] 1 AC 247, at para 31, Lord Bingham, contemplating the possibility that authority to publish might have been refused without adequate justification (or at any rate where the former member firmly believed that no adequate justification existed), said: "In this situation the former member is entitled to seek judicial review of the decision to refuse, a course which the OSA 1989 does not seek to inhibit." In that case, however, the disclosures had been made before the enactment of RIPA and the creation of the IPT and it is plain that the House had not been referred to section 65(2)(a), still less had had occasion to consider its scope. It cannot sensibly be supposed that the case would have been decided any differently had it been recognised that after 2 October 2000 such a challenge would have had to be brought before the IPT.

29 Admittedly the *Esbester* line of cases were decided in the context of article 8 (rather than article 10) and, understandably, Strasbourg attaches particular weight to the right to freedom of expression. Neither A nor JUSTICE, however, were able to show us any successful article 10 cases involving national security considerations save only for *Sunday Times v United Kingdom (No 2)* (1991) 14 EHRR 229 (*Spycatcher*) where, of course, the disputed material was already in the public domain.

30 For my part I am wholly unpersuaded that the hearing of A's complaint in the IPT will necessarily involve a breach of article 6. There is some measure of flexibility in the IPT's rules such as allows it to adapt its procedures to provide as much information to the complainant as possible consistently with national security interests. In any event, of course, through his lengthy exchanges with B, A has learned in some detail why objections to publication remain. Article 6 complaints fall to be judged in the light of all the circumstances of the case. We would, it seems to me, be going further than the Strasbourg jurisprudence has yet gone were we to hold in the abstract that the IPT procedures are necessarily incompatible with article 6(1). Consistently with the well known rulings of the House of Lords in *R (Ullah) v Special Adjudicator* [2004] 2 AC 323, para 20 and *R (Al-Skeini) v Secretary of State for Defence (The Redress Trust intervening)* [2008] AC 153, paras 105, 106, I would decline to do so, particularly since, as already mentioned, the IPT's own decision on its rules is shortly to be considered by the ECtHR.

31 Over and above all this is the further and fundamental consideration, that even if the IPT's Rules and procedures *are* in any way incompatible with article 6, the remedy for that lies rather in *their* modification than in some artificially limited construction of the IPT's jurisdiction. It is, indeed, difficult to understand which of the appellant's

A contended-for constructions is said to be advanced by this submission. On any view the IPT has *some* jurisdiction. Yet the argument involves a root and branch challenge to its procedures in *all* cases.

(iii) Anomalies

32 The Court of Appeal's construction of section 65(2)(a) is said to give
B rise to a number of anomalies. Under this head I shall touch too upon certain other points advanced variously by A and JUSTICE.

33 The first anomaly is said to be that while section 7(1)(a) HRA proceedings have to be brought before the IPT, other causes of action or public law grounds for judicial review need not. This point troubled Rix LJ who asked, ante, p 18, para 39: "what is so special about section 7
C proceedings under the 1998 Act against the intelligence services . . . ?" The answer surely is that such claims are the most likely to require a penetrating examination of the justification for the intelligence services' actions and, therefore, close scrutiny of sensitive material and operational judgment. But it may well be (as, indeed, Rix LJ foresaw) that section 65(2)(d) of RIPA will be brought into force so that the Secretary of State can allocate other proceedings too exclusively to the IPT. Meantime, subject always to the
D court's abuse of process jurisdiction and the exercise of its discretion in public law cases, proceedings outside section 7(1)(a) can still be brought in the courts so that full effect is given to the preservation of such rights by section 11 of HRA.

34 It is similarly said to be anomalous that whereas A, responsibly seeking prior clearance for the publication of his manuscript, is driven into
E the IPT, someone in a similar position, although perhaps facing injunctive proceedings for having sought to publish without permission, would be entitled pursuant to section 7(1)(b) HRA to rely in those ordinary court proceedings on their article 10 rights. Whilst I readily see the force of this, the answer to it may be that defences were not sufficiently thought through at the time of this legislation and that more, rather than fewer, proceedings involving the intelligence services should be allocated exclusively to the IPT.

F 35 A further anomaly is said to be that Special Branch police officers and Ministry of Defence special forces may well carry out work of comparable sensitivity to that undertaken by the intelligence services and yet section 7(1)(a) HRA claims brought against them would proceed in the ordinary courts and not in the IPT. Part of the answer to this is to be found in "the special position of those employed in the security and intelligence
G services, and the special nature of the work they carry out" (Lord Bingham's opinion in *R v Shayler* [2003] 1 AC 247, at para 36); the rest in the same response as to the earlier points: perhaps the IPT's exclusive jurisdiction should be widened.

36 Sitting a little uneasily alongside the last suggested anomaly is the contention that section 65(2)(a) vests in the IPT exclusive jurisdiction over various kinds of proceedings against people quite other than the intelligence
H services which may involve little if anything in the way of sensitive material—for example, pursuant to section 65(3)(c), proceedings under section 55(4) of RIPA with regard to accessing encrypted data. Whatever view one takes about this, however, it is impossible to see how it supports either of the alternative constructions of section 65 for which A contends.

37 In short, none of the suggested anomalies resulting from the Court of Appeal's construction seems to me to cast the least doubt on its correctness let alone to compel some strained alternative construction of the section.

38 I see no reason to doubt that the IPT is well able to give full consideration to this dispute about the publication of A's manuscript and, adjusting the procedures as necessary, to resolve it justly. Quite why A appears more concerned than B about the lack of any subsequent right of appeal is difficult to understand. Either way, Parliament has dictated that the IPT has exclusive and final jurisdiction in the matter. I would dismiss the appeal.

LORD HOPE OF CRAIGHEAD DPSC

39 I agree with Lord Brown of Eaton-under-Heywood JSC's opinion. I wish only to add a few brief footnotes.

The Rules

40 As Lord Brown JSC has explained (see para 14, above), among the factors that reinforce the conclusion that is to be drawn from the terms of the statute that Parliament did not intend to leave it to the complainant to choose for himself whether to bring his proceedings in a court or before the IPT are the provisions that RIPA contains about the rules that may be made under it. In *Hanlon v The Law Society* [1981] AC 124, 193–194 Lord Lowry set out the circumstances in which a regulation made under a statutory power was admissible for the purpose of construing the statute under which it was made. The use of the rules themselves as an aid to construction, in addition to what RIPA itself says about them, needs however to be treated with some care.

41 In *Deposit Protection Board v Dalia* [1994] 2 AC 367 the issue was as to the meaning of the word "depositor", and the regulations that were prayed in aid were made four years after the date of the enactment. At p 397, Lord Browne-Wilkinson said that regulations could only be used an aid to construction where the regulations are roughly contemporaneous with the Act being construed. In *Dimond v Lovell* [2000] QB 216, para 48 Sir Richard Scott V-C said that he did not think that the content of regulations which postdated the Consumer Credit Act 1974 by some nine years could be taken to be a guide to what Parliament intended by the language used in the Act. One must also bear in mind, as Lord Lowry said in *Hanlon's* case [1981] AC 124, 193–194, that Regulations cannot be said to control the meaning of the Act, as that would be to disregard the role of the court as interpreter.

42 In this case the statute received the Royal Assent on 28 July 2000. The Investigatory Powers Tribunal Rules 2000 were made on 28 September 2000 and laid before Parliament the next day. The interval was so short that, taken together, they can be regarded as all part of same legislative exercise. But, as Mr Crow for B submitted, it is not the content of the Rules as such that matters here. Rather it is the fact that the Act itself put a specialist regime in place to ensure that the IPT was properly equipped to deal with sensitive intelligence material. Section 68(4) of RIPA limits the information that the tribunal may give to a complainant where they determine any complaint brought before them to a statement that a determination either has been or has not been made in the complainant's favour. Section 69(4)

states that the Secretary of State's power to make rules under that section includes power to make rules that limit the information that is given to the complainant and the extent of his participation in the proceedings. Section 69(6)(b) states that in making rules under that section the Secretary of State shall have regard in particular to the need to secure that information is not disclosed to an extent that is contrary to the public interest or prejudicial to national security.

43 The fact that this regime was so carefully designed to protect the public interest by the scheme that is set out in the statute is in itself a strong pointer to the conclusion that Parliament did not intend by section 65(2)(a) that the jurisdiction of the IPT in relation to claims of the kind that A seeks to bring in this case was to be optional. I do not think that it is necessary to go further and look at the Rules themselves, as the indication that the statute itself gives is so clear on this point.

Anomalies

44 Although he adopted a different stance before Collins J, as the judge recorded in para 20 of his opinion [2009] 4 All ER 511, A now accepts that the legal challenge that he is making to B's decision is properly to be characterised as proceedings under section 7(1)(a) of the Human Rights Act 1998 and not under section 7(1)(b) of that Act. Section 7(1)(a) of the 1998 Act provides that a person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may "bring proceedings against the authority under this Act in the appropriate court of tribunal". Section 7(1)(b) provides, in the alternative, that he may "rely on the Convention right or rights concerned in any legal proceedings".

45 As *Clayton & Tomlinson, The Law of Human Rights*, 2nd ed (2009), para 22.03, puts it:

> "This section contemplates two ways in which a person may advance a contention that a public authority has acted in a way which is incompatible with his Convention rights: either by making a *free standing* claim based on a Convention right in accordance with section 7(1)(a) or by *relying* on a Convention right in proceedings in accordance with section 7(1)(b)."

In *R v Kansal (No 2)* [2002] 2 AC 69, 105–106 I said that section 7(1)(a) and section 7(1)(b) are designed to provide two quite different remedies. Section 7(1)(a) enables the victim of the unlawful act to bring proceedings under the Act against the authority. It is intended to cater for freestanding claims made under the Act where there are no other proceedings in which the claim can be made. It does not apply where the victim wishes to rely on his Convention rights in existing proceedings which have been brought against him by a public authority. His remedy in those proceedings is that provided by section 7(1)(b), which is not subject to the time limit on proceedings under section 7(1)(a) prescribed by section 7(5); see also *Wilson v First County Trust Ltd (No 2)* [2004] 1 AC 816, para 90. The purpose of section 7(1)(b) is to enable persons against whom proceedings have been brought by a public authority to rely on the Convention rights for their protection.

46 The fact that section 65(2)(a) requires proceedings under section 7(1)(a) to be brought before the IPT, while relying on section 7(1)(b) was not

subject to this requirement, was said by Mr Millar to be anomalous. Why, he said, should a claim be so restricted when a defence relying on Convention rights to injunctive proceedings by a public authority, or a counterclaim, was not? I am reluctant to conclude that the omission of a reference to section 7(1)(b) was due to an oversight, and I do not think that when regard is had to the purpose of these provisions there is any anomaly.

47 I would reject the suggestion that a counterclaim against a public authority on the ground that it has acted (or proposes to act) in a way that is made unlawful under section 6(1) of the 1998 Act should be regarded as having been made under section 7(1)(b). This issue is not to be resolved by reference to the procedural route by which the claim is made but by reference to the substance of the claim. A counterclaim against a public authority for a breach of Convention rights is to be treated as a claim for the purposes of section 7(1)(a): see section 7(2) which states that proceedings against an authority include a counterclaim or similar proceedings. It will be subject to the time limit on proceedings under that provision in section 7(5).

48 As for defences, the scheme of the 1998 Act is that a person who is (or would be) a victim of an act that it is made unlawful by section 6(1) because the public authority has acted (or proposes to act) in that way is entitled to raise that issue as a defence in any legal proceedings that may be brought against him. Section 7(1)(b) contemplates proceedings in which it would be open to the court or tribunal to grant relief against the public authority on grounds relating to a breach of the person's Convention rights, such as those guaranteed by article 6. The scope for inquiry is relatively limited in comparison with that which may be opened up by a claim made under section 7(1)(a).

49 It is possible, however, to envisage a situation in which a defence to an application for injunctive relief by the intelligence services would open up for inquiry issues of the kind that section 65(2)(a) of RIPA reserves for determination by the IPT if they were to be subject of a claim under section 7(1)(a), the disclosure of which would be contrary to the public interest or prejudicial to national security. It is true that the legislation does not address this problem, perhaps because it was thought inappropriate to reserve to the IPT proceedings that were initiated by and in the control of the intelligence services or any other person in respect of conduct on their behalf. But the situation that this reveals is, I think, properly to be regarded as a product of the way the legislative scheme itself was framed. It does not provide a sound reason for thinking that Parliament intended to leave it to the complainant to choose whether to bring *his* proceedings in a court rather than before the IPT.

50 Like Lord Brown, I can find nothing in this alleged anomaly, or in any of the others that have been suggested, that supports the construction of section 65(2)(a) for which A contends.

Appeal dismissed.
Claimant to pay half director's reasonable costs in House of Lords and Supreme Court, to be assessed if not agreed.

SH

Statement No 1
For the Respondents
Dated 16 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT/14/85/CH
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT/120-126/CH
BETWEEN:

GREENNET LIMITED
RISEUP NEWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

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

Respondents

WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1. I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

2. I am authorised to make this witness statement on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.

3. Attached to this statement and marked Exhibit ['CM1'] is a bundle of relevant documents. Tab and page numbers below are references to that Exhibit.

4. In this statement I use the term "the intelligence services" to refer, collectively, to the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. I also use the terms "MI5", "SIS" and "GCHQ" to refer to those bodies individually.

5. In this statement I will (I) address the current intelligence picture and the ongoing challenges posed by changes in technology and developments in the communications market, (II) provide an overview of Computer and Network Exploitation (CNE) and its importance and value in fulfilling GCHQ's statutory functions, before (III) addressing some key safeguards and oversight mechanisms for CNE activities carried out by GCHQ, including:

a) The processes for applying for warrants under section 5 of the Intelligence Services Act 1994;
b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
c) Oversight by the Intelligence Services Commissioner, a retired senior judge;
d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

I. THE CURRENT INTELLIGENCE PICTURE

6. The intelligence background to the preliminary issues of law in the *Liberty/Privacy* proceedings was set out in paragraphs 8 to 19 of the witness statement dated 16th May 2014 of Charles Farr, Director General of the Office for Security and Counter Terrorism (OSCT) at the Home Office. I adopt and agree with that statement of the background as it then stood. Given the passage of time, it is necessary to update it and I do so below.

7. Over the past year, the threat to the UK from international terrorism in particular has continued to increase. On the 17 September 2015, Andrew Parker, the Director General of the Security Service (MI5), during an interview with the BBC, revealed that six alleged terror plots targeting the UK have been stopped in the preceding twelve months during an interview with the BBC. In August 2014, the UK threat level, assessed independently by the Joint Terrorism Analysis Centre ("JTAC"), was raised to "SEVERE" from "SUBSTANTIAL", which means that an attack in the UK is highly likely. The principal terrorist threat to the UK continues to derive from militant Islamist terrorists, particularly in Syria and Iraq, where the Islamic State of Iraq and the Levant ("ISIL") has emerged as the most violent of the terrorist groups operating in that region.

8. The recent 2014 Annual Report by the Home Office on the UK's Counter-Terrorism Strategy ("the CONTEST Report"), published on 23 March 2015, highlights the increase in the frequency of terrorist incidents around the world, and the number of fatalities associated with such attacks [CM1-1]. In 2013 (the latest year for which published statistics are available) there were nearly 12,000 terrorist attacks in 91 countries – 40% more than in 2012. These resulted in more than 22,000 fatalities. Just over half of all attacks occurred in three countries: Iraq, Afghanistan and Pakistan. As the Report explains:

"The principal threat continues to come from militant Islamist terrorists, notably in Syria and Iraq. ISIL and other terrorist groups in Syria are now supported by foreign fighters from the UK and other European countries. About 6000 people with extremist connections are among the many Britons who have travelled to the region from the UK. Many have now returned here. Some are likely to have received combat experience and other terrorist related training. Terrorism is being fuelled by an unprecedented quantity of extremist and terrorist propaganda."

9. The murder of two British and other hostages in Syria, apparently by a member of ISIL closely connected to the UK, recent terrible events in Paris and Copenhagen and the 31 Britons killed in the attacks of March and June on a Tunisian museum and beach resort, have underlined the threat posed to British nationals – not just in Syria or Iraq but also outside those arenas, including within the EU. In response to the increase in the UK threat level the Government legislated in 2014 to strengthen the UK's capabilities and provided an uplift in counter-terrorism funding including £130m of additional counter-terrorism funding.

10. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging and it is one in which GCHQ plays a leading role given its expertise in digital communications technology. The evolution of the internet and modern forms of communications are providing terrorists and criminals with new ways to plan direct and increasingly execute their plots. The CONTEST Report notes that ISIL in particular is using social media "…. in an unprecedented quantity and frequency, including personalised messages from UK and other foreign fighters and propaganda from the organisation." As Andrew Parker, the Director General of the Security Service (MI5) explained in a public speech to the Royal United Services Institute (RUSI) on 8 January 2015 [CM1-2]:

"It makes full use of the modern social media and communications methods through which many of us now live our lives. By these means it spreads its message of hate directly in to homes across the United Kingdom – both to those seeking it and those who may be susceptible to its distortion and glamorisation of horrific acts".

11. Robert Hannigan, the Director of GCHQ also drew attention in November 2014 to the way in which ISIL is using the internet to "create a jihadi threat with near-global reach" [CM1-3]. In particular:

"[ISIL] also differs from its predecessors in the security of its communications. This presents an even greater challenge to agencies such as GCHQ. Terrorist have always found ways of hiding their operations. But today mobile technology and smartphones

have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are "Snowden approved". There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years."

12. The diversification of the communications market and the ability of terrorists, criminals and others to exploit new internet-based technologies has made it increasingly difficult for GCHQ and the other intelligence services to monitor the communications of those who present a threat to UK interests. Unless the intelligence services are able to maintain their capabilities in the face of these unprecedented technological challenges, the UK will be unable to obtain the intelligence it needs to counter these threats. As the Chief of SIS made clear in his speech to English Heritage in March 2015, the intelligence services are engaged "... in a technology arms race" **[CM1-4]**.

13. Mr Parker, the Head of MI5, discussed the changing nature of the challenges that the intelligence services face in his BBC interview of 17 September 2015 **[CM1-6]**:

"We need to be able to use data sets so we can join the dots, to be able to find and stop the terrorists who mean us harm before they are able to bring the plots to fruition. We have been pretty successful at that in recent years but it is becoming more difficult to do that as technology changes faster and faster."

14. The threat to the UK does not stem just from terrorism. For example, as David Anderson QC noted in his independent report on investigatory powers, *A Question of Trust*, **[CM1-7]**, GCHQ used analysis of bulk data to track down two men overseas who had been harnessing the vulnerabilities of the web to blackmail hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. It was the vital work of GCHQ analysts that brought this abuse to an end: they were able to confirm the suspects' names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.

15. But this work tackling national security threats in the digital age is getting harder. One important challenge is the implication of the use of encrypted communications. Encryption is important for computer security and GCHQ advocates its use in the UK as part of good cyber security practice. But the rise of encryption offered by telecommunications companies to their customers has impacted particularly severely on GCHQ's intelligence capabilities because encrypted data acquired lawfully by GCHQ may be unreadable to the intelligence services. The challenges posed by the growth of encryption have become particularly acute over the course of the last two years as telecommunications companies increasingly use improved privacy protections, including encryption by default, as part of their marketing strategies. According to the Director of Europol encryption has now become **[CM1-8]**:

"... the biggest problem for the police and the security service authorities in dealing with the threats from terrorism... It's changed the very nature of counter-terrorist work from

one that has been traditionally reliant on having good monitoring capability of communications to one that essentially doesn't provide that anymore."

16. The US authorities have experienced similar problems relating to the growth of encryption which they refer to as "Going Dark". The Director of the FBI recently explained [CM1-9]:

"Encryption just isn't a technical feature, it's part of a marketing pitch, but it will have very serious consequences for law enforcement and national security agencies at all levels...There should be no law-free zones in this country..."

17. In a public speech given to RUSI on 10 March 2015, the Foreign Secretary offered a summary of the challenges posed by the accelerating pace of technological change [CM1-10]:

"And as the range of threats gets bigger, so the pace of technological change with which the Agencies must keep pace is getting faster, making their central task of keeping us safe ever more demanding. The Agencies have always had to innovate to stay one step ahead of their adversaries. But the accelerating pace of technological change has upped the ante as terrorists, states and others who would do us harm embrace, adapt, and abuse the technology that we so readily welcome in our everyday lives.

And it is a truism that as technology enables greater productivity, it also open us up to greater vulnerability. So our Agencies must master every technological advance. They must understand its strengths, its weaknesses, the vulnerabilities it introduces – before our enemies can turn it against us".

18. The Security and Intelligence Agencies Financial Statement of June 2014 recognises that the need to maintain capabilities in the face of these rapid technological changes is perhaps the greatest challenge currently faced by the intelligence services [CM1-11].

19. David Anderson QC also highlighted the impact of these challenges in his annual report of the Terrorism Acts (September 2015) [CM1-12]:

"It has been a feature of several major terrorist attacks, including the 7/7 bombings, the killing of Lee Rigby and the French shootings in January 2015, that one or more of the perpetrators was known to the police or security services but had not been assessed as posing a major risk at the time. The speed with which things can change, and the difficulties in knowing how best to prioritise limited surveillance resources, were illustrated in unprecedented detail by the inquiry of Parliament's Intelligence and Security Committee into Lee Rigby's killing."

20. The age of ubiquitous encryption means, inter alia, that GCHQ and the other intelligence agencies require a more innovative and agile set of technical capabilities to meet the serious national security challenges of the digital age. Computer and Network Exploitation (CNE) is one such capability. CNE operations have been authorised by senior Ministers for many years since the 1994 Act, but its importance relative to GCHQ's overall capabilities has been increasing significantly in recent years and is likely to increase further. The allegations made in both claims concern activities known by the

intelligence services as CNE, so it is necessary to describe in more detail what CNE operations are.

II. AN OVERVIEW OF CNE AND ITS IMPORTANCE AND VALUE

Computer and Network Exploitation ("CNE")

21. CNE is a set of techniques through which an individual gains covert and remote access to a computer (including both networked and mobile computer devices) typically with a view to obtaining information from it. GCHQ carries out CNE operations as part of its intelligence-gathering activities, as set out below.

22. CNE operations vary in complexity. A straightforward example is the use of the login credentials of a target to gain access to the data held on a computer. The login credentials could belong to a normal user or an entity with elevated privileges such as an administrator.

23. More sophisticated CNE operations involve taking advantage of weaknesses in software. For instance a piece of software may have a "vulnerability": a shortcoming in the coding that may permit the development of an "exploit", typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerability in order to cause unintended or unanticipated behaviour to occur. This unanticipated behaviour might include allowing another piece of software – an implant, sometimes called a "backdoor" or a "Trojan" - to be installed on the device.

24. The exploit and subsequent implant can be delivered in a number of ways. Two of the techniques are:

    a) The user of a device might be sent an e-mail inviting them to open a link or document of interest. When the user clicks on the link or document, it takes them to website that delivers the implant. This is known as "phishing".

    b) Alternatively, an individual with access to a computer might insert the implant using, for example, a USB stick, whether wittingly or otherwise.

25. The function of an implant may also vary in complexity. A simple implant will typically explore the target computer, sending back information over the internet to its controller. Others might monitor the activity of the user of the target device, or take control of the computer.

26. As with interception, there are a range of circumstances in which a state may require its intelligence services 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 enables the state to obtain the valuable intelligence it needs to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

27. CNE operations may enable GCHQ to obtain communications and data of individuals who are engaged in activities that are criminal or harmful to national security. Such circumstances may arise where, for example:

    a) the fact that the wanted communications were not in the course of their transmission and could not therefore be intercepted;

    b) the absence of any Communications Services Providers (CSPs) on whom a warrant can be served to acquire particular communications; and

    c) the greater possibility of acquiring a comprehensive set of the target's communications/data by means of CNE.

Importance and value of CNE

28. As discussed above, CNE is a critical tool in the investigation of threats to the UK. The UK Government does not have the same ability to identify individuals and entities outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ's capabilities are the key sovereign intelligence-gathering capabilities available to the Government.

29. Historically, GCHQ's ability to identify individuals of intelligence interest has been based largely on bulk interception. This capability remains critical to the identification and mitigation of threats, but increasingly it is being threatened by the unprecedented technological challenges outlined in part (I) of my statement. As the Foreign Secretary explained in his speech to RUSI:

    "...And to GCHQ, although since its birth a signals intelligence organisation, the rapid pace of the development of the internet and the sheer scale of its traffic, pose new challenges – finding the needle of vital information to safeguard our security in a hay stack that is growing exponentially and is already well beyond the capacity of human analysis."

30. As noted in the previous section, the introduction of strong encryption across many web services in the wake of the Snowden allegations has posed particular technological challenges. The spread of encryption has impeded intelligence service access to communications. In his own speech to RUSI on "terrorism, technology and accountability, Andrew Parker, the Director General of MI5 said:

    "Changes in the technology that people are using to communicate are making it harder for the Agencies to maintain the capability to intercept the communications of terrorists. Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced."

31. In the light of these developments, CNE is increasingly required to enable GCHQ to continue to obtain the intelligence the Government requires to identify individuals outside the UK who may pose a threat to national security. Indeed CNE may in some cases be the only way to acquire intelligence coverage of a terrorist suspect or serious

criminal in a foreign country. As noted by the Intelligence and Security Committee at page 67 of its Privacy and Security Report [CM1-13]:

"During 2013 a significant number of GCHQ's intelligence reports contained information that derived from IT operations against a target's computer or network....."

32. At the same time as GCHQ is adapting to meet these new technological challenges, there is an increasing expectation within Government that GCHQ will play a lead role in improving cyber security for the protection of the UK's vital national interest in an era where threats to the UK from cyber space are growing very rapidly. GCHQ plays a key role in securing the safety of the internet for the benefit of the public as I explain further below. CNE is an important part of GCHQ's ability to understand, detect and disrupt cyber threats to the UK.

33. GCHQ's CNE capabilities have made a vital contribution to counter the increased threat to the UK from militant Islamist terrorists. And, as noted in the previous section, GCHQ's CNE capabilities have also enabled the disruption of paedophile-related crime. I cannot say more about these operations in this open, public statement without undermining the interests of national security and the prevention and detection of serious crime.

34. CNE has long been an essential part of GCHQ's capabilities. It has become increasingly important in recent years and will become more important yet in the years ahead. Without it, GCHQ's ability to protect the public from terrorism, cyber attack, serious crime, including child sexual exploitation, and a range of other threats would be seriously degraded.

The Claimant's allegations about CNE

35. The Claimants make a number of general and specific allegations in the two Claims. Before addressing the specific allegations made by the Complainants, I would like to make four preliminary points in relation to the general allegations.

36. First, the Claimants allege that the tools used by GCHQ allow huge amounts of information (current and historical) to be extracted from "millions" of devices thereby subjecting users to mass and intrusive surveillance. Allegations that GCHQ conducts "mass surveillance" were made by one of the Claimants in the context of a previous complaint before this Tribunal. On that occasion the Tribunal stated "we are entirely clear that the Respondents are not seeking, nor asserting that the system entitles them to seek, to carry out what has been described as "*mass*" or "*bulk*" surveillance". I should like to make clear that it is equally the case that GCHQ neither seeks, nor believes that we are entitled to seek to carry out indiscriminate mass surveillance activities of the sort alleged in this case. They are also precluded by the clear statutory framework which regulates GCHQ's activities. CNE must be authorised by a Secretary of State and is subject to strict tests of necessity, proportionality and legitimate aim as set out in the Intelligence Services Act 1994. These authorisations, and the internal processes that GCHQ has in place to manage the authorised activities, are subject to independent scrutiny by the Intelligence Services Commissioner. In February 2015, the Government published a draft Equipment Interference Code of Practice. It set out the strong

safeguards that GCHQ has always applied to CNE activities. More generally, any conduct by GCHQ must be consistent with its statutory functions and the purposes for which those functions may be exercised. As the ISC has recently made clear in its report on Privacy and Security:

"We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do."

37. It follows that a significant proportion of the examples given in the Claimants' evidence with respect to the possibilities created by CNE tools bear no relation to the reality of GCHQ's activity and/or would be unlawful having regard to the relevant statutory regime.

38. Secondly, the Claimants allege that CNE may create potential security vulnerabilities or leave users vulnerable to further damage.

39. Intelligence work by its nature is secret – both the how and the specific targets. It is therefore in GCHQ's interests to carry out CNE operations in such as way that the activity is not apparent to the target, nor to others wanting to know who the specific targets of HMG intelligence activities are. GCHQ does not intrude into privacy any more than is necessary to discharge our functions. Nor would it be right to enable others to intrude into privacy. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. It would also increase the risk of those who wish to know who our targets are identifying GCHQ's tools and techniques. Operations are therefore carried out in such a way as to minimise that risk.

40. I should also like to take this opportunity to explain GCHQ's role more generally in securing the safety of the internet for the benefit of the public. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes. PwC's 2015 Information security breaches survey [CM1-5] reported that 90% of large organisations and 74% of small businesses had a security breach in the period covered by the report; the average cost of the worst serious breach ranged from £1.46m to £3.14m for large organisations; £75,000 to £311,000 for small businesses. GCHQ's role is to play its part in helping to make the internet as safe as possible for ordinary citizens and legitimate businesses, and prevent its use by criminals and terrorists. We engage with strategically important organisations who are particularly vulnerable to cyber attack, and we also promote high standards of cyber security across all sectors of the UK, including by recommending the use of strong encryption.

41. One element of GCHQ's information assurance work concerns the finding and reporting of vulnerabilities in digital technologies. GCHQ helps technology providers identify weaknesses in finished hardware and software; we also help uncover potential issues at the design stage, often before they become major in-service problems – saving firms time and money. Some but not all vendors choose to publicly credit GCHQ for finding those weaknesses. For example, in September of this year, Apple publicly credited CESG, the Information Security arm of GCHQ, with the detection of a vulnerability in their iOS operating system which could have been exploited to allow the unauthorised modification of software on devices such as iPhones and iPads, the extraction of information from

those devices, or to disrupt their operation. That vulnerability has now been patched. In the last two years, GCHQ has disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business.

42. Thirdly, while CNE operations can be highly intrusive, they are not in general any more intrusive than any other operations conducted by GCHQ under the Regulation of Investigatory Powers Act 2000 ("RIPA") or the Intelligence Services Act 1994 ("ISA").

43. By way of example, Part II of RIPA permits certain public authorities to authorise intrusive surveillance in relation to residential premises and private vehicles. A listening device located within a private address - potentially including a bedroom – clearly has the potential to obtain private information relating to all the occupants of that address (including non-targets) of an extremely sensitive and personal nature. Information of this nature which is communicated between two or more people within a residential address or a private vehicle may well contain content that those individuals would deem too personal, private or sensitive to commit to writing and store on a device. Nonetheless, such highly intrusive surveillance is lawful if properly authorised, having met the tests of necessity and proportionality.

44. Similarly, while CNE operations can be used to access a wide range of data, they are not in general any more intrusive than the interception of communications under Chapter I of Part I of RIPA. With the advent of Cloud storage (which many people opt to use), all the material referred to by the Claimants in their complaints would be potentially available to the intercepting agencies via interception – including photographs, videos, passwords, banking details, passport details, etc. All of this material could, in principle, be acquired by way of interception.

45. In summary, while the level of intrusiveness will clearly vary depending on the type of activity in issue, I do not therefore believe it is the case that GCHQ's CNE operations are in general any more intrusive than its other operations involving interception, surveillance or other investigative techniques.

46. Fourthly and finally, GCHQ recognises that CNE activity could theoretically change the material on a computer. For example the installation of an implant would itself amount to a change. However it would be neither necessary nor proportionate, nor would it be operationally sensible, for an organisation seeking to use CNE for intelligence gathering purposes to make more than the most minimal, and to the greatest extent possible, transient, changes to targeted devices.

III. SAFEGUARDS AND OVERSIGHT MECHANISMS

Overview

47. The regime governing GCHQ's CNE activities consists of provisions in primary legislation and in relevant Codes of Practice and also in relevant internal arrangements and safeguards which are applied by GCHQ.

48. I explain below the key components of the application process for CNE warrants and authorisations, and the oversight arrangements governing GCHQ's CNE activities. These processes are supplement by the Equipment Interference Code of Practice **[CM1-14]** which contains important safeguards including:

a) Detailed guidance on the requirement of proportionality and the considerations which apply in the CNE context, including issues such as collateral intrusion and the need to consider less intrusive alternatives (Chapter 2);
b) Guidance on the frequency of reviews, particularly where there is a high level of intrusion into private life or significant collateral intrusion or confidential information is likely to be obtained (Chapter 2 at §§2.13-2.15);
c) Best practice guidance on applications for warrants/authorisations (§§2.16-2.17);
d) Special considerations which should apply to legally privileged and confidential information (Chapter 3);
e) Detailed and comprehensive procedures for the authorisation of both sections 5 and 7 ISA equipment interference activity (see Chapters 4 and 7);
f) Important record keeping requirements in respect of any CNE (Chapter 5);
g) Comprehensive safeguards and guidance as regards the processing, retention, disclosure, deletion and destruction of any information obtained by the intelligence services pursuant to interference CNE warrant, which mirror similar safeguards applied as part of the interception regime pursuant to section 15 of RIPA (Chapter 6).

49. GCHQ's internal arrangements are safeguards set out in the Respondents' Closed Response and Closed witness evidence. I also refer to certain of the internal arrangements in this statement. They include the Compliance Guide, which is a document which is made available electronically to all GCHQ staff. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity be:

a) Authorised (generally through a warrant or equivalent legal authorisation);

b) Necessary for one of GCHQ's operational purposes; and

c) Proportionate.

49A. These principles and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

49B. In addition, pursuant to GCHQ's Compliance Guide and Intelligence Sharing and Release Policy (a policy document governing the sharing and release of operational data), the position is that all operational warrant is handled, disclosed and shared as

though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

49C. GCHQ's internal arrangements also address the role of the Reporting Quality Checker in ensuring that any release of intelligence outside of GCHQ is lawful and proportionate.

49D. GCHQ has a collaborative relationship with the NSA. Activities forming part of that relationship must be undertaken in accordance with the principles set out in the Compliance Guide, which emphasises the need for all operational activity to be necessary and proportionate.

Authorising CNE: section 5 and 7 ISA

50. GCHQ conducts all CNE activity pursuant to warrants under section 5 of the ISA or authorisations under section 7 of the ISA. I have set out below an explanation of the differences between the section 5 ISA regime and the section 7 ISA regime as it applies to GCHQ's activities. I have also identified the detailed safeguards which regulate this activity including:

a) The processes for applying for, renewing and cancelling section 5 warrants;
b) The processes for gaining section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
c) Oversight by the Intelligence Services Commissioner;
d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

51. These safeguards and oversight mechanisms are reflected in the Covert Surveillance and Property Interference Code and the draft Equipment Interference Code of Practice

a) The processes for applying for section 5 warrants

52. The section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. Section 5(2) of ISA provides that the Secretary of State may, on an application made by GCHQ, issue a warrant authorising the taking of action in respect of property as specified in that warrant if he: thinks it necessary for the action to be taken for the purpose of GCHQ in carrying out any function that falls within section 3(1)(a) of ISA; is satisfied that the taking of action is proportionate to what the action seeks to achieve; and is satisfied that satisfactory arrangements are in force under section 4(2)(a) of ISA 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.

53. Applications for section 5 warrants in respect of CNE must contain all the detailed matters as set out in paragraph 4.6 of the current draft Equipment Interference Code of Practice. Prior to the publication of this draft Code of Practice on 5 February 2015 applications were required to conform with paragraph 7.37 of the Covert Surveillance and Property Interference Revised Code of Practice published on 10 December 2014 **[CM1-15]**. This required GCHQ to provide the same information in support of an application as

would be required when the police, the services police, National Crime Agency (NCA), HM Revenue and Customs (HMRC) or Competition and Markets Authority (CMA) were making an application to an authorising officer. The details of this information are set out in paragraph 7.18 of the Surveillance and Property Interference Revised Code of Practice. These requirements (and the numbers of the relevant paragraphs) were unchanged from previous versions of the Code of Practice published in [2000] and revised in 2010.

53A. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its use."

53B. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). This was updated in January 2015. The internal guidance is regularly reviewed to ensure that it remains comprehensive and pertinent as GCHQ's CNE activities continue to evolve. The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals

The importance of CNE as an overseas intelligence gathering capability

54. As I have already explained, the UK Government does not have the same ability to identify individuals outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ's capabilities are the key sovereign intelligence-gathering capabilities available to the Government.

55. There are important practical differences between gathering intelligence on individuals, organisations and equipment within the UK and gathering intelligence on individuals, organisations and equipment that exist or operate outside that jurisdiction. These

practical differences are reflected in the authorisation regimes provided by sections 5 and 7 of the ISA.

56. As mentioned above, the section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. By contrast, section 7 permits the giving of class authorisations which do not require the authorisation to name or describe a particular piece of equipment, or an individual user of the equipment. Consequently CNE is authorised in relation to equipment located outside the UK pursuant to a section 7 class authorisation and internal approvals. This reflects practical realities of intelligence gathering outside the UK, where GCHQ requires the flexibility to obtain material which will contain intelligence relevant to the safeguarding of the UK's national security without knowing in advance from which particular piece of equipment that material may be obtained.

57. In line with the foregoing, a class authorisation under section 7 ISA is sought wherever members of GCHQ conduct CNE in relation to equipment located outside the UK that would otherwise be unlawful. This includes cases where the act is done in the UK , but is intended to be done in relation to apparatus that is or is believed to be outside the UK, or in relation to anything appearing to originate from such apparatus. In addition GCHQ will obtain a section 7 authorisation for any CNE activities carried out abroad or over a foreign computer, even if the relevant user is located in the UK. Paragraph 7.4 of the current draft Equipment Interference Code of Practice sets out the additional safeguards which apply if either the subject of a section 7 operation is known to be in the UK, or the equipment is brought to the UK during the currency of the authorisation.

58. While GCHQ's section 7 CNE class authorisation offers the potential for broader and more flexible acquisition of intelligence than is permitted under its section 5 warrants, the process described below for giving section 7 authorisations, in combination with GCHQ's system of internal approvals and additions, ensures that its activities are properly regulated and subject to strict safeguards and oversight.

Section 7 authorisations

59. Section 7 ISA provides that an authorisation has to be issued personally by the Secretary of State on an application to him to that effect. The purposes for which warrants are issued are set out in section 7(3) ISA.

60. Section 7(1) of ISA provides that a person shall not be liable in the United Kingdom for any act done outside the UK for which he would be liable, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under that section.

61. Paragraph 7.1 of the current draft Equipment Interference Code of Practice requires that GCHQ applies the provisions of that Code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of ISA. Paragraph 7.7 of the current draft Equipment Interference Code of Practice states that an application for the giving or renewal of a section 7 authorisation should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 CNE warrant.

62. Paragraph 7.11 of the current draft Equipment Interference Code of Practice states that an authorisation under section 7 may relate to a broad class of operations. Paragraph 7.12 states that where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of CNE must be sought from a designated senior official. In any case where the CNE activity may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer (and in the case of GCHQ an Annex A approving Officer is someone in a small group of GCHQ's most senior managers).

63. Applications for section 7 authorisations must, as far as is reasonably practicable in the circumstances, contain all the detailed matters set out in paragraph [4.6] of the EI Code. The process by which GCHQ obtains Secretary of State authorisation for class authorisations under section 7 of the ISA has evolved over the last few years with an increasing emphasis on providing detailed information to the Secretary of State about the type of CNE activities covered by the class authorisation. Since July 2014 GCHQ has copied to the FCO all of its internal section 7 approvals for CNE operations which were given pursuant to the class authorisation. In August 2013 GCHQ recommended that, in future, the internal approvals should be sent through the relevant department in the FCO to the Secretary of State and this was agreed by the FCO.

Internal approvals

64. Where a class authorisation has been given by the Secretary of State under section 7, internal Approval to conduct individual operations under that authorisation in respect of CNE must also be sought from a designated senior official.

65. Before granting an approval, the senior official must be satisfied that the proposed operations are necessary, proportionate and within the scope of the class authorisation. Approval may only be given where operations are necessary in the interests of national security, for the prevention and detection of serious crime or in the interests of the economic wellbeing of the UK. In addition, the senior official must be satisfied that the nature and degree of the proposed intrusion against target computers is proportionate and limited to that required for the operation to be effective, and that safeguards are in place to ensure that any aspect of the operation or the data thus obtained is handled in a manner consistent with GCHQ's legal obligations under Intelligence Services Act and the Human Rights Act. Feeding into the internal approvals process is an internal specialist risk assessment panel, involving a range of relevant technical, operational and policy leads. This panel provides expert oversight and assurance to operators, policy leads and senior leadership that the tools and techniques being used, and the way in which they are being used, present an acceptable level of technical and operational risk. Key agreements and decisions made by the internal specialist risk assessment panel are documented. They provide an audit trail and a 'history' of decisions (which, for example, are used to inform risk assessment statements made in section 7 approval requests and political submissions).

66. GCHQ copies to the Foreign and Commonwealth Office all of its internal s.7 approvals and extensions for CNE implant operations which were given pursuant to the class

authorisation. In addition, if an operation is judged to present significant risk, the proposal will be submitted to FCO officials or the Secretary of State (and GCHQ will also seek FCO legal advice if a proposed operation involves issues of international law).

66A. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an "addition" to an existing approval is required.

Additions

67. Under an internal approval, operations against specific targets are authorised by means of an 'addition'. The term "addition" is not specifically defined in GCHQ's internal arrangements, but is used within GCHQ to refer to the process and associated formal documentation for the inclusion of further specific targets within the scope of an existing internal approval for a CNE operation. The "additions form" requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

68. The level of detail in an addition will be tailored to the operation in question, but it will describe the specific target (which must fit within the description of the target set in the relevant internal approval) and the necessity and proportionality of the planned operation, as well as how intrusion into privacy will be managed. The addition will also describe the planned activity and assess the risks associated with this (which must fit within the thresholds set in the relevant internal approval). The role and seniority of the authoriser for additions depends on factors including the sensitivity and complexity of the planned activity, but the authoriser must always have been trained before assuming the role.

68A. Analysts will have assigned to them a point of contact within the CNE operational team with whom they can speak about operational matters. In addition, within their own team they will have a dedicated point of contact with whom they can discuss any legal and policy questions.

Records

68B. GCHQ creates and maintains records of the application for, renewal of, approval of and cancellation of all warrants under section 5 and class authorisations and internal approvals under section 7 indefinitely. These include any comments or stipulations from the Secretary of State relating to them.

Training

68C. GCHQ has a comprehensive programme of training and testing in place for those involved in CNE operations and for intelligence analysts who may have access to data obtained in CNE operations. This training includes operational and mandatory legalities training. The training involves testing and regular reassessment.

c) Oversight by the Intelligence Services Commissioner

The Commissioner

69. GCHQ's CNE operations are overseen by the Intelligence Services Commissioner under section 59(1) of RIPA. The Rt Hon Sir Mark Waller currently holds this role and he was appointed by the Prime Minister on 1 January 2011. His predecessor was Sir Peter Gibson (also a former Lord Justice of Appeal).

70. The functions of the Intelligence Services Commissioner, as they relate to CNE, are:

a) To keep under review the exercise by the Secretary of State of his powers to issue, renew and cancel warrants under sections 5 and 6 of ISA;
b) To keep under review the exercise by the Secretary of State of his powers to give, renew, and cancel authorisations under section 7 of ISA;
c) To give the Tribunal all such assistance (including my opinion on any issue falling to be determined by it) as it may require in connection with its investigation, consideration or determination of any matter;
d) To make an annual report to the Prime Minister on the carrying out of my functions, such report to be laid before Parliament.

71. The Intelligence Services Commissioner formally inspects GCHQ's CNE activity twice a year, and also makes ad hoc visits to look at particular aspects of its work in more depth. These are known as 'under the bonnet' visits. During the formal inspections the Commissioner raises inquiries, examines procedures and examines the relevant paperwork for a selection of warrants, class authorisations (including internal approvals and relevant additions), that he personally has chosen in advance, to ensure that it is in order and that, in particular, sufficient consideration has been given to issues like collateral intrusion and privacy. In order to permit the Commissioner to make a selection of the documents he wishes to see, GCHQ provides him with a "choice letter" containing:

a) Summaries of all section 5 ISA warrants and section 7 ISA class authorisations that are either in place or which have been cancelled or allowed to expire since the previous choice letter, including all internal approvals underneath the latter. Those warrants and class authorisations that the Commissioner has previously inspected are flagged as such;
b) A list of errors reported to the Commissioner since the previous Review;
c) A list of intelligence reports at least partially sourced from CNE operations, which contain confidential or legally privileged material issued since the previous choice letter;
d) A list of all warrants and authorisations examined at previous reviews by the current Commissioner.

71A. As part of the **September 2010** visit, Sir Peter Gibson discussed a recently reported CNE error which led to a change being made in warrant applications.

71B. During Sir Mark Waller's visit in **March 2011** he commented on the section 7 approvals and noted that 'proportionality' appeared in its own right on the section 7 approval form, but would have liked to see 'necessity' appear in its own right on the form. This change was subsequently introduced.

71C. During the **December 2013** Inspection the Commissioner expressed himself content with the actions GCHQ had taken in respect of documenting privacy considerations in warrant and authorisation application paperwork since June 2013.

71D. Following the discovery of a typographical error relating to the expiry date of the renewal of a section 5 warrant the Commissioner had asked that the Secretary of State amend the face of the instrument in his own hand and initial the change. The Commissioner queried why the error had not been picked up sooner and asked to see a copy of the checklist that is used to check warrants before they go up to FCO. He asked that the list be supplemented with a further check to be carried out when the signed warrant is returned from the warrant issuing department to ensure that any future mistakes are picked up at an early stage. He also asked to be informed if there were any similar instances in the future and this was agreed.

71E. There was also a discussion of what information should be included on warrant renewal instruments. It was explained that, until recent years, renewal instruments for section 5 warrants had contained the minimum wording stipulated by ISA section 6. GCHQ had subsequently added a description of the property (which made it easier to see to what a renewal instrument referred), and, prompted by the Commissioner, had then added a final paragraph reminding the Secretary of State of his statutory obligations when signing the renewal. The Commissioner's view was sought as to whether it would be helpful to add a description of the actions authorised by the warrant. Sir Mark felt that, if we were minded to make further changes to the renewal instrument, we might consider including all the relevant wording from the original instrument.

71F. In **the May 2014** Inspection the Commissioner recommended a new form of words for section 5 warrants which make clear that the Secretary of State is authorising on the basis that GCHQ will act in accordance with the accompanying submission. He also made recommendations about the conditions set out in the submissions and instruments. He continued to monitor thematic property warrants closely.

71G. In the **November 2014** Inspection the Commissioner expressed himself content that GCHQ record on the warrant instrument that we will comply with any conditions set out in the accompanying submission as this formally joins the warrant to the submission.

71H. There was also discussion about section 5 ISA warrants that are "thematic" rather than relating to specific property. The Commissioner asked that section 5 warrants should relate to specific property wherever possible rather than relying on a thematic warrant. Overall the Commissioner indicated that he was content for such warrants to be used, where there is no intrusion into privacy, but emphasised that they should be the exception and not the rule.

71I. The Commissioner's **April 2015** Inspection was the first inspection at which the Commissioner formally inspected the Additions layer (under internal approvals) for the s.7 authorisations process. As already set out above, this is the layer at which individual targets are usually described. The Commissioner recommended changes be

made to ensure that each element is dealt with explicitly and at the earliest opportunity. These changes have been implemented.

71J. Sir Mark Waller has conducted a number of what he refers to as "under the bonnet" visits, separate from his formal inspections.

a) On 20 January 2012 Sir Mark was briefed on GCHQ's CNE activities.

b) On 10 July 2013 Sir Mark sat in on one of the legalities courses.

c) On 11 September 2014 Sir Mark visited GCHQ following an approach to him by a BBC journalist, following media reports about certain alleged CNE activities.

71K. The Commissioner's most recent "under the bonnet" visit was on 9 December 2014. This visit was intended to give him an overview of GCHQ's operational use of CNE so that he could see how our internal governance processes meshed with the authorisation regime. During the visit we established that Sir Mark fully understood the section 5 authorisation regime, so the focus was primarily on operational activity authorised under ISA s.7, and how GCHQ used its internal hierarchy of approvals and additions. Sir Mark was briefed on the internal approvals process, and the circumstances where GCHQ would seek political approval for activities.

71L. I am aware that the Intelligence and Security Committee of Parliament, in their report of 12 March 2015, "Privacy and Security: A modern and transparent legal framework", addressed section 7 authorised operations at paragraphs 177ff and said this at Recommendation BB on page 66:

"While intrusive action within the UK requires a Ministerial warrant, outside the UK it is authorised by the use of a Class Authorisation under the Intelligence Services Act 1994. However, the Agencies do not all keep detailed records of operational activity conducted under these Class Authorisations. It is essential that they keep comprehensive and accurate records of when they use these powers. It is unacceptable not to record information on intrusive action."

Given the Commissioner's clear endorsement of GCHQ's internal section 7 processes and the associated record keeping undertaken by GCHQ (the "audit trail" in the Commissioner's words), I do not consider that this statement relates to GCHQ's CNE operations. As set out earlier in this statement GCHQ does keep very detailed records of CNE activity cconducted pursuant to section 7 authorisations, including all details of internal Approvals and Additions.

71M. Finally, it is to be noted that we have an established process for reporting errors to the Commissioner. In particular error reports follow a standard structure with sections addressing:

- The background;
- How and why was it identified?
- What was the magnitude of the error?
- Why did this happen?
- How we'll make sure it never happens again.

Reports of the Commissioner

72. In his formal reports, the Commissioner has explained the extent of his oversight of GCHQ's CNE activities and made a number of positive comments about GCHQ's CNE operations and the thoroughness of its processes. In his report for 2013 **[CM1-20]** the commissioner stated:

"From my work it is clear to me that GCHQ apply the same human rights considerations and the same privacy considerations, checks and balances to the virtual world as they do to the real world. From my scrutiny of GCHQ authorisations, inspection visits and my under the bonnet work, it is my view that GCHQ staff continue to conduct themselves with the highest level of integrity and legal compliance."

72A. In his Report for 2014 **[CM1-16]** the Commissioner explained the nature of his review functions and highlighted the extent of co-operation which he received from the Agencies in this regard. He stated:

"I emphasise that I do this activity personally and I undertake my duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves, without political favour or personal bias..."

"A duty of cooperation is imposed on every member of every agency, every departmental official and every member of the armed forces to disclose or provide to me all such documents and information as I may require. I have never had anything but cooperation in this regard."

72B. In the same report he commented on GCHQ's record keeping in terms of warrantry and authorisation:

"GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips."

72C. The Commissioner also noted that he had spent a day at GCHQ looking at the system by which GCHQ manages its internal approvals and additions, and questioning the staff who undertake the approvals and the CNE activity, in order to understand what consideration was being given at each stage of the process to protecting privacy, and what was done with any product from CNE operations. The Commissioner concluded:

"My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration that was given to each operation; it was clear to me that a great deal of thought was going into the process..."

"GCHQ primarily operate under class authorisations and have very few specific section 7s. They provide for my oversight the internal approvals they make under each class authorisation and have implemented my recommendation to ensure that the paperwork reflects that these approvals are only valid as long as the class authorisation is in place. They are approved by a GCHQ senior official but if there is any additional sensitivity or

political risk it will only be signed after a senior Foreign Office official or the Foreign Secretary has been consulted and agreed the operation is appropriate. I have made it clear that the senior official cannot authorise necessity and proportionality; this decision must be made by the Secretary of State and cannot be delegated."

"GCHQ's internal approvals are supplemented by what they call an "addition". To help me gain a better understanding I spent a day in GCHQ:
- Looking more closely at the system;
- Questioning the staff who undertake the approvals; and
- Questioning the staff who undertake the activity."

"I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion."

"I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I recommended that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ."

73. This recommendation has been implemented.

d) Oversight by the Intelligence and Security Committee of Parliament

The Committee

74. GCHQ is responsible to the Secretary of State for Foreign and Commonwealth Affairs. The Secretary of State is in turn accountable to Parliament. Parliamentary responsibility for scrutiny of the activities of GCHQ falls principally to the Intelligence and Security Committee of Parliament ("the ISC").

75. The ISC, in its original form, was established by the Intelligence Services Act 1994. On 25 June 2013 the ISC was reconstituted under the Justice and Security Act 2013 ("the JSA"). From that date onwards the JSA has provided the governing statutory framework for the ISC. In its annual report for 2012-2013 [CMI-17], the ISC stated that it welcomed the changes in the JSA and that those changes were "broadly in line with those which we ourselves had previously recommended to the Government, and which will increase accountability" (at page 83).

76. The ISC operates within the "ring of secrecy" which is protected by the Official Secrets Act 1989. It may therefore consider classified information, and in practice takes oral evidence in open and closed session from the Foreign and Home Secretaries, the three heads of the intelligence services, and their staff.

77. The heads of the intelligence services are under a general obligation to arrange for any information requested by the ISC in the exercise of its functions to be made available to it. The power to refuse such a request has been removed from the heads of the

intelligence services and now lies with Ministers alone, who can only exercise this power in certain limited circumstances.

78. In order to be able effectively to carry out its expanded remit under the JSA, the ISC's budget has been substantially increased and the ISC is in the process of recruiting further staff. This will result in a three-fold increase in the ISC's investigative capacity.

Privacy and Security: A modern and transparent legal framework

79. The ISC sets its own agenda and work programme. Following the Snowden allegations in the summer of 2013, the ISC decided to investigate an allegation made in some of those reports to the effect that GCHQ had acted illegally by accessing communications content via the US PRISM programme. On 17 July the Committee made a statement **[CM1-18]** which concluded that the allegation that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications was unfounded. They also concluded that it would nevertheless be proper to "... consider further whether the current statutory framework governing access to private communications remains adequate."

80. On 17 October 2013, the ISC announced that it would be broadening this review of the legislative framework governing the intelligence services' access to the content of private communications to consider, additionally, the appropriate balance between privacy and security in an internet age **[CM1-19]**. The result of this review, Privacy and Security: A modern and transparent legal framework, was published on 12 March 2015 **[CM1-13]**. Paragraph v of the introduction to the review says:

"Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities, including how they are used, the legal framework that regulates their use, the authorisation process, and the oversight and scrutiny arrangements that apply."

81. The Committees first key finding reads:

"We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do."

82. In the report the Committee also indicated that it had been informed about the full range of Agency capabilities, how they are used and how they are authorised.

Conclusion

83. In this statement I have endeavoured to the best of my ability and knowledge to:

- describe the range of serious national security threats faced by the UK and its people to which GCHQ is required to assist in defending against;

- set out the requirement for Computer and Network Exploitation (CNE) capabilities to help us counter these threats, principally international terrorism, cyber attack (including from hostile state actors), and serious crime (including child sexual exploitation);

- give an account of the robust procedures for the use of GCHQ's CNE capabilities, and summarise the result of various Parliamentary, judicial and other inquiries and inspections which shows GCHQ's adherence to these strict procedures;

- describe the growing importance of CNE to the protection of the UK. Whilst it has been an important GCHQ capability for many years, its importance has been growing and is set to grow further, partly because of the growth of ubiquitous encryption which has affected GCHQ's ability to collect data for intelligence purposes by other means. It is therefore the case that without CNE capabilities GCHQ's ability to protect the British public from terrorism, cyber attack, online child sexual exploitation and a range of other serious crime would be badly diminished.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: .....

Dated: 16 November 2015

Statement No 2
For the Respondents
Dated 23 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/14/85/CH**
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/120-126/CH**
BETWEEN:

GREENNET LIMITED
RISEUP NEWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

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

Respondents

SECOND WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1) I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also have wider responsibilities for GCHQ's external communications and policy. I have been in

this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

2) This is my second witness statement in these proceedings which I am authorised to make on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.

3) Attached to this statement and marked Exhibit **['CM2']** is a bundle of relevant documents. Tab and page numbers below are references to that Exhibit.

4) In this second statement I address GCHQ's safeguards for communications protected by legal professional privilege ("LPP") and other confidential communications.

LPP and confidential communications

5) The RIPA Interception of Communications Code of Practice and the draft Equipment Interference Code of Practice stipulate that particular consideration should be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information (such as that which is legally privileged) is involved. GCHQ therefore takes special care to ensure that the acquisition, analysis and retention of communications in these circumstances, and the dissemination of any intelligence produced from them, is necessary and proportionate.

6) GCHQ treats four main categories of material as requiring special handling and dissemination; material that is legally privileged, confidential personal information, confidential journalistic information and the communications of and with UK legislators.

7) GCHQ applies those safeguards and handling procedures in place to ensure compliance with the RIPA Interception of Communications Code of Practice to all its data, irrespective of origin. Therefore, GCHQ's policies are applicable across the board, and apply equally to data derived from Computer Network Exploitation (CNE) as they do to data derived from other forms of interception.

8) A number of different GCHQ policies are relevant to the interception of legally privileged communications.

9) Acting on the advice of Counsel to Her Majesty's Government (HMG), and following the Belhaj IPT complaint, GCHQ's policies on the interception and reporting of legally

privileged communications were updated in the first half of 2015. In June 2015 the Interception of Communications Commissioner's Office (IOCCO) was consulted on these changes, and by August 2015 the policies had been further amended to incorporate suggestions made by IOCCO.

10) A copy of the 'Targeting' section of GCHQ's Compliance Guide is attached at [**CM2-1**]. This contains guidance where there may be targeting of lawyer's communications. This requires that "careful consideration" is given where lawyer-client communications are targeted. The 2015 changes to the policies on the interception and reporting of legally privileged communications stipulate that if officers intend to carry out any targeting that may attract any of the four categories of sensitive communications, (including those of a lawyer), an internal authorisation (a Combined Policy Authorisation (COPA)) must be obtained. In particular, where legally privileged information is or is likely to be involved, this authorisation must be ratified by a senior Foreign and Commonwealth Office (FCO) official prior to its approval within GCHQ.

11) Further information is provided in the 'Communications containing Confidential Information' section of the Compliance Guide (see attached at [**CM2-2**]). This document contains stipulations which are necessary in order to comply with the requirements of the Code of Practice where material which is legally privileged may be intercepted. This makes expressly clear that no material should be transcribed, gisted or otherwise analysed unless there are reasonable grounds to believe that it is necessary on the grounds of national security, the economic well-being of the UK or preventing or detecting a serious crime (see page 3 of [**CM2-2**]). It also states that intelligence based on the interception of confidential information can only be disseminated in accordance with GCHQ Reporting Policies on the sensitive professions and proportionality. Any intelligence that may potentially be confidential must be submitted for mandatory sensi-check. Staff other than those in the relevant GCHQ team are not empowered to release such information themselves unless as per agreement with the relevant GCHQ team.

12) As of April 2015 it specifies in the 'Communications containing Confidential Information' section of the Compliance Guide that if officers are likely to obtain confidential information as a result of their targeting activities, they must obtain a COPA in advance. This directive reasserts that in the case of legally privileged information, the COPA must be ratified by a senior FCO official.

13) The 'Oversight' section of the Compliance Guide (see [**CM2-3**]) explains that both the Intelligence Services Commissioner and the Interception of Communications Commissioner have oversight of the Intelligence Agencies' activities in respect of the four categories of communications containing confidential information, as specified above. Warrants and reporting that relate to communications containing confidential information will explicitly be

brought to the attention of the relevant Commissioner during the next inspection visit. Any material containing confidential communications that is retained will be made available to the relevant Commissioner if requested, including detail of whether that material has been disseminated.

14) GCHQ's Intelligence Sharing and Release Policy (see **[CM2-4]**) which came into force in September 2013 and was updated in June 2015 contains further guidance on the RIPA Code of Practice, the Human Rights Act 1998 and confidential communications. This document explains legal privilege and makes clear that such communications attract a special sensitivity. Any such material must undergo a mandatory sensitivity check (referred to as a sensi-check in the guidance). This check is done by a team separate from the team dealing with reporting. If in a particular case it is proportionate to release legally privileged material, the reporter will be instructed to apply the following caveat to the report, to help demonstrate that GCHQ has taken account of the communications' sensitivity and the heightened threshold of proportionality:

> *"This report contains material that may be subject to legal professional privilege, and onward dissemination/Action On is not to be taken without reverting to GCHQ."*

15) The Intelligence Sharing and Release Policy sets out how the process of sensi-checking should be conducted. It also makes clear makes clear that communications of, and as of 2015, mention of sensitive professionals including lawyers or legal advisers are subject to a mandatory sensi-check. Prior to the creation of the Intelligence Sharing and Release Policy in September 2013, the equivalent policy was to be found in "Reporting Policy – Sensitive Professions" (see **[CM2-5]**) which applied between December 2010 and September 2013 and in Repnotes 27 and 28 (see **[CM2-6]**) which applied between 2005 and December 2010. The changes to the policy on the interception and reporting of legally privileged communications in the first half of 2015 brought with it a lowering of the threshold for sensi-check for the reporting of privileged material. Presently, all reporting that mentions a lawyer must be submitted to sensi-checkers, who will refer a high number of these reports to Legal Advisers. Formerly, only reporting on the communications of a lawyer went via this route. As a result of the implementation of the 2015 policy and process amendments, the amount of reporting referred by sensi-checkers to Legal Advisers to ascertain whether or not the contents of an intelligence report carries legal privilege or not has arisen.

16) The "Sensi-Checking: How To Guide" (see **[CM2-7]**), contains a separate section on legal privilege. This makes clear that reporters and reporting quality checkers are not qualified or permitted to decide whether:

a) the communications are privileged – this is reserved to Legal Advisers (LA) or to sensi-checkers or

b) reporting the privileged communications is necessary and proportionate – this is reserved to sensi-checkers (acting on legal advice if appropriate).

17) Further it is made clear that the act of sensi-checking any such reporting is not sufficient to meet the Code of Conduct and it is vital that the additional consideration required is given and recorded. This is followed by a step by step guide to identifying whether the material is privileged which is used by sensi-checkers; guidance on the sending of reports to Legal Advisers; guidance on the reporting of such material including whether caveats should be added to the report and guidance on sensi-check exceptions (where the subject happens to be a lawyer but where the information obtained from them is routinely not privileged). The current version of the "Sensi-Checking: How To Guide" is dated March 2015 and the previous version of that Guide was last updated in December 2013.

18) Legally privileged material is not shown to lawyers engaged in relevant litigation. The practice underpinning this, known as Information Barriers, is set out in **[CM2-8]**. It is awaiting formal approval by the relevant GCHQ senior official. However, this policy has been followed in practice across the department since the Belhaj ruling, and reflects longstanding practice before that date.

19) As of June 2015, the Review and Retention section of the Compliance Guide states that material that contains legally privileged or other confidential information, or directly involves British Parliamentarians, and that is not required for intelligence reporting purposes must be deleted as soon as practicable, and that requests for exceptional retention of such material are unlikely to be approved. Following the Belhaj ruling, GCHQ made changes to the arrangements for the retention of legally privileged material. Prior to the Belhaj claim, non-reissued intelligence reports were retained in GCHQ's intelligence report repository along with all other intelligence reports. Following Belhaj, GCHQ has taken steps to ensure the isolation of any legally privileged intelligence reports which have been retained in the repository and do not meet the threshold for onward reporting by GCHQ to its customers. GCHQ now intends to institute routine isolation and deletion on a rolling basis; intelligence reports will continue to exist in the intelligence report repository for six months in order to give all relevant analysts the opportunity to assess the relevance of the intelligence. After this time non-reissued legally privileged intelligence reports will be moved into isolation and will become subject to strict access controls. These isolated intelligence reports will be routinely deleted on a rolling monthly basis.

20) I also attach (see **[CM2-9]**) an up-to-date summary of GCHQ's policy and guidance in relation to the special protection afforded to legally privileged information and other especially sensitive communications.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: .....

Dated: 23 November 2015

Statement No 3
For the Respondents
Dated 24 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/14/85/CH**
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/120-126/CH**
BETWEEN:

GREENNET LIMITED
RISEUP NEWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

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

Respondents

THIRD WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1) I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also

have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

2) This is my third witness statement in these proceedings which I am authorised to make on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.

3) In this third statement I respond to certain statements in the Claimants' evidence.

Claimants' evidence

Professor Anderson

4) At §§21-23 of Professor Anderson's evidence he asserts that the intrusion which occurs during CNE activities "may place lives at risk" and he cites an example of political opponents hacking servers in hospitals in Oregon which interfered with medical equipment and put lives at risk.

5) GCHQ's CNE activities are carefully monitored, planned, authorised and inspected. We can only use any of our capabilities when it is necessary and proportionate to do so. So, whilst CNE, like a very broad range of other human activity, can put lives at risk if conducted in a reckless and irresponsible way, putting the lives of innocent members of the public at risk is not acceptable to GCHQ. GCHQ never carries out reckless and irresponsible CNE operations. That would be unlawful and we do not do it.

6) Additionally, GCHQ's processes for CNE include an expert risk assessment panel. This is referred to in my first statement at §65.

Eric King

7) In terms of the scale of CNE operations (see §§136-141 of Mr King's statement), GCHQ cannot confirm or deny assertions regarding the scale of its operations. However, it is simply not correct to assert that GCHQ is using CNE on an indiscriminate and disproportionate scale. As discussed at §28 of my first statement, CNE is a critical GCHQ tool.

Professor Sommer

8) I would not accept Professor Sommer's criticism of the CNE Code on the basis that the type of activity which is involved is too imprecise (see §11ff of his statement). The definitions in §1.6 of the Code do broadly reflect the type of CNE which is conducted and it is to be noted that the Ministerial Foreword to the Consultation Document published with the Code also gave further detail including that it applies to different investigative techniques (i.e. different from interception) including "the use of computer network exploitation, to identify, track and disrupt the most sophisticated targets."

9) Nor would I accept his statement about the role of Ministers. Professor Sommer asserts that politicians have an insufficient understanding of the methods which are employed, e.g. by GCHQ, in the CNE field, such that they are unable properly to assess necessity and proportionality when authorising warrants/authorisations under s.5 and s.7 ISA.

10) It is our responsibility within GCHQ to make sure that we explain the nature of our proposed activity and the intelligence requirements for it so that those who have to authorise the activity can do so on a fully informed basis. It is for that reason that we provide detailed information in support of the s.5 and s.7 warrants/authorisations, as required under the CNE Code. In terms of the CNE Code, it is to be noted that following the public consultation process, the Equipment Interference Code of Practice was laid before Parliament on 4 November 2015. However the paragraphs and paragraph numbers referred to in this and my previous statement are unaltered.

11) This detailed information is then given serious attention by senior Ministers and their advisers. In respect of s.5 and s.7 warrants/authorisations, the FCO has a unit headed at Director General level which, inter alia, advises the Foreign Secretary on authorisation applications. Part of this process involves seeking advice from the department's lawyers, whose views are reflected directly. Meetings to discuss individual warrants/authorisations, and/or requests for further information, and/or requests for different options, are common. As such, Ministers engage very significantly in the detail of the authorisations process and scrutinise carefully the methods that are employed.

12) As to the issues raised at §§96.2 and 108-111 of Professor Sommer's statement, there are precautions which are applied where there is any risk that CNE activities may have the potential to affect evidence in future criminal prosecutions.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: .....

Dated: 24 November 2015