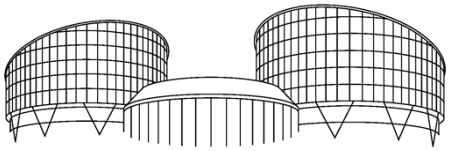

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

DECISION

This version was rectified on 4 September 2020 under Rule 81 of the Rules of Court.

Application no. 46259/16
PRIVACY INTERNATIONAL and Others
against the United Kingdom

The European Court of Human Rights (First Section), sitting on 7 July 2020 as a Committee composed of:

Aleš Pejchal, *President,*
Pauliine Koskelo,
Tim Eicke, *judges,*

and Renata Degener, *Deputy Section Registrar,*

Having regard to the above application lodged on 5 August 2016,

Having regard to the observations submitted by the respondent Government and the observations in reply submitted by the applicants,

Having regard to the comments submitted by six third party intervenors: the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, L. Roussey and French Data Network, Mozilla Corporation, La Quadrature du Net, Electronic Privacy Information Center, and Article 19,

Having deliberated, decides as follows:

THE FACTS

1. A list of the applicants is set out in the appendix.

The British Government ("the Government") were represented by their Agent, Mr C. Wickremasinghe.

A. The circumstances of the case

2. The facts of the case, as submitted by the parties, may be summarised as follows.

3. The first applicant, Privacy International, is an NGO registered in London. The second applicant, GreenNet Limited, is an Internet service provider registered in London. The third applicant, Chaos Computer Club E.V., is an association of "hacktivists" registered in Germany. The fourth and fifth applicants, Media Jumpstart Inc. and Riseup Networks Inc., are companies registered in the United States providing Internet services and communications services respectively. The sixth applicant, Korean Progressive Network Jinbonet, is an Internet service provider registered in South Korea.

4. The applicants believe that their equipment has been subject to interference known as Computer Network Exploitation or Equipment Interference, to say colloquially "hacked", over an undefined period by the United Kingdom Government Communications Headquarters ("GCHQ") and/or the Secret Intelligence Service ("SIS"). They consider that GCHQ and/or SIS obtained authorisations to conduct that Equipment Interference under section 7 of the Intelligence Services Act 1994 ("ISA"). Section 7 allows the Secretary of State to authorise a person to undertake (and to exempt them from liability for) an act outside the British Islands in relation to which they would be liable if it were done in the United Kingdom (see paragraph 25 below).

5. In part iv of his Annual report for 2015 the Intelligence Services Commissioner described Equipment Interference thus:

> "...
>
> Equipment Interference (EI) is any interference, remotely or otherwise, with computers, servers, routers, laptops, mobile phones and other devices in order to obtain information from the equipment. Information obtained may include communications content and communications data, and information about the equipment to allow an intelligence service to examine or modify the equipment, or to conduct surveillance.
>
> ..."

6. Privacy International considers the belief it has been subject to Equipment Interference to be reasonable because it is an organisation which campaigns against unlawful State surveillance. The other applicants consider their belief reasonable because they have access to the communications of many individuals, or because their employees have access to source code or other software of interest to the United Kingdom Government.

1. The Investigatory Powers Tribunal

7. The applicants complained to the Investigatory Powers Tribunal (the "IPT") that they had been subject to Equipment Interference and that this was in breach of domestic law and in violation of Articles 8 and 10 of the Convention. In those proceedings they complained about being subject

to Equipment Interference both inside and outside the United Kingdom. The IPT held a hearing which lasted for three days during which it heard argument from the parties' legal representatives and took evidence from expert witnesses. It gave its judgment on 12 February 2016.

8. At the outset of its decision the IPT explained its well-established approach to:

> "2. ... make assumptions as to the significant facts in favour of claimants and reach conclusions on that basis, and only once it is concluded whether or not, if the assumed facts were established, the respondent's conduct would be unlawful, to consider the position thereafter in closed session. This procedure has enabled the Tribunal on what is now a number of occasions, to hold open inter partes hearings, without possible damage to national security, while preserving, where appropriate the Respondents proper position of Neither Confirmed Nor Denied."

9. The proceedings went ahead on the basis of an assumption in favour of the applicants and were not held in closed session at any point. In the course of the proceedings the Government accepted (or avowed) the use of Equipment Interference. They also published the Equipment Interference Code of Practice (see paragraphs 26-27 below).

10. Examining first the domestic legal regime, the IPT concluded that acts of Equipment Interference which would be unlawful under the Computer Misuse Act 1990 ("CMA" – see paragraphs 22-23 below), were rendered lawful where a warrant or authorisation to conduct Equipment Interference had been obtained under sections 5 or 7 of the ISA, respectively.

11. Having considered domestic lawfulness, the IPT turned expressly to the Convention arguments and set out its conclusions concerning section 7 authorisations (in relation to acts done outside the British Islands) in paragraphs 53 and 63 of its decision.

12. It considered first the question of jurisdiction and whether Equipment Interference undertaken outside the United Kingdom would come within the scope of the Convention.

13. The IPT noted that there was no possibility to issue a code of practice for section 7 but that the Equipment Interference Code of Practice itself indicated:

> "49 ... SIS and GCHQ should as a matter of policy apply the provisions of [the] code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands."

14. The IPT observed however that the Code included a footnote which said it was "without prejudice as to arguments regarding the applicability of the ECHR". The IPT went on to recall that section 7 authorised unlawful acts "outside the British Islands". It contrasted this with the member states' obligation to secure to everyone "within their jurisdiction" the rights and freedoms set out in the Convention. With reference to the Court's case-law

it observed that jurisdiction under the Convention is accordingly territorial and it is only in exceptional circumstances that extraterritorial jurisdiction arises.

15. The IPT then noted the parties' agreement that in ordinary circumstances there would be no jurisdiction and, in cases where someone who is the subject of a section 7 authorisation is abroad, it would be difficult to argue that such a person is within the territorial scope of the Convention and there would be a very limited number of circumstances in which there was going to be a breach of the Convention.

16. The parties also agreed that it might be in some circumstances that an individual claimant could claim a breach of their Article 8 or 10 rights as a result of a section 7 authorisation but that did not mean that the section 7 regime as a whole was non-compliant with those Articles. The IPT concluded on the question of jurisdiction by reserving its position, commenting:

> "53 ... we reserve for future consideration if and when particular facts arise and the position of jurisdiction to challenge a s.7 warrant can be and has been fully argued, whether an individual complainant may be able to mount a claim ... we have an insufficient factual basis to reach any useful conclusion."

17. The IPT then turned to examine the complaint about "bulk CNE [Equipment Interference]". So far as it concerned the section 7 regime the IPT concluded with reference to what was then future legislation (see paragraphs 29-31 below):

> "62. Both aspects of Mr Jaffey [the claimants representative]'s complaints appear to have been taken up in the IP Bill. Under the heading "BULK POWERS" in the accompanying Guide, it is stated, at paragraph 42, that where the content of a UK person's data, acquired under bulk interception and bulk equipment interference powers, is to be examined, a targeted interception or equipment interference warrant will need to be obtained. As for the question of presence in the British Islands, it is specifically provided in draft clause 147, within the Chapter dealing with "Bulk Equipment Interference Warrants", namely by clause 147(4), that there is to be a similar safeguard to that in s.16 of RIPA in relation to the selection of material for examination referable to an individual known to be in the British Islands at the time.
>
> 63. It seems to us clear that these criticisms are likely primarily to relate to Bulk CNE carried out, if it is carried out at all, pursuant to a s.7 authorisation (hence paragraph 7.4 of the E I Code). Mr Jaffey's own example was of the hacking of a large internet service provider in a foreign country, and the diversion of all of the data to GCHQ, instead of intercepting that material "over a pipe" which might be encrypted, so as to render access by ordinary bulk interception difficult if not impossible. As with Issue 5 [scope of the Convention], Mr Jaffey specifically accepted (Day 2/46) that, if Bulk CNE were taking place, and if, prior to any changes such as discussed above, there were to be insufficient safeguards in place, that does not render the whole CNE scheme unlawful. As with Issue 5, we reserve for consideration, on particular facts and when questions of jurisdiction are examined, whether an individual complainant might be able to mount a claim."

18. The IPT then considered the question whether the section 5 regime (in relation to acts mainly done inside the United Kingdom) was compliant with Article 8 of the Convention before and after the publication of the Equipment Interference Code in February 2015 during (and apparently as a result of) the proceedings. Before doing so it underlined that in light of its conclusions concerning jurisdiction under section 7 (see paragraphs 12-13 above), there was no need for it to examine the section 7 regime but that in any event the answer would be the same in relation to the question whether the section 5 regime is compliant with the Convention as for section 7. It then went on to examine the section 5 regime and following a close examination of this Court's case-law concluded that it had been compliant with the Convention both before and after the publication of the Code.

19. The IPT summarised its conclusions thus:

> "89. ...
>
> (i) Issue 1 [S.10 of the CMA]: An act (CNE) which would be an offence under s.3 of the CMA is made lawful by a s.5 warrant or s.7 authorisation, and the amendment of s.10 CMA was simply confirmatory of that fact.
>
> (ii) Issue 2 [Territorial jurisdiction in respect of ss.5/7]: An act abroad pursuant to ss.5 or 7 of the ISA which would otherwise be an offence under ss.1 and/or 3 of the CMA would not be unlawful.
>
> ...
>
> (v) Issue 5 [Scope of the Convention]: There might be circumstances in which an individual claimant might be able to claim a breach of Article 8/10 rights as a result of a s.7 authorisation, but that does not lead to a conclusion that the s.7 regime is non-compliant with Articles 8 or 10.
>
> ...
>
> (vii) Issue 7 [Bulk CNE]: If information were obtained in bulk through the use of CNE, there might be circumstances in which an individual complainant might be able to mount a claim, but in principle CNE is lawful.
>
> (viii) Issue 8 [S.5 post-February 2015 (Weber ...4) to (6)]: The s.5 regime since February 2015 is compliant with Articles 8/10.
>
> (ix) Issue 9 [S.5 prior to February 2015]: The s.5 regime prior to February 2015 was compliant with Articles 8/10.
>
> ...
>
> 90. The use of CNE [Equipment Interference] by GCHQ, now avowed, has obviously raised a number of serious questions, which we have done our best to resolve in this Judgment. Plainly it again emphasises the requirement for a balance to be drawn between the urgent need of the Intelligence Agencies to safeguard the public and the protection of an individual's privacy and/or freedom of expression. We are satisfied that with the new [Equipment Interference] Code and whatever the outcome of the Parliamentary consideration of the IP Bill, a proper balance is being struck in regards to the matters we have been asked to consider."

20. On 9 March 2016 the IPT sent the applicants a "no determination letter" which read as follows:

"The Investigatory Powers Tribunal has carefully considered your clients' complaints and Human Rights Act claims in the light of all relevant evidence and in accordance with its normal procedures. The Tribunal has asked me to inform you that no determination has been made in your favour either on your complaints or your Human Rights Act claims.

...

For the avoidance of doubt the Tribunal has not been required to consider, and has not considered, the matters left open in paragraphs 53 and 63 of the Privacy/Greennet judgment."

21. The first applicant brought a claim for judicial review[1] of the decision of the IPT so far as it concerned section 5 of the ISA. That litigation is currently pending before the High Court[2] (see paragraphs 32-33 below).

B. Relevant domestic law and practice

1. The Computer Misuse Act 1990

22. Sections 1 and 3 of the Act make unlawful unauthorised access to computer material, and unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computers etc. According to the IPT, an act of CNE would constitute an offence under sections 1 and 3 of the Act.

23. Section 10 of the Act was amended on 3 May 2015 to expressly provide that a person acting under a warrant or authorisation granted under section 5 or 7 respectively of the Intelligence Services Act 1994 (see paragraphs 24-25 below) does not commit an offence.

2. The Intelligence Services Act 1994

24. Section 5 (1) of ISA reads as follows:

"5. Warrants: general.

No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section."

25. Section 7 (1) of ISA reads as follows:

"7. Authorisation of acts outside the British Islands.

If apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section."

[1] Rectified on 4 September 2020: "appealed" was replaced by "brought a claim for judicial review of".
[2] Rectified on 4 September 2020: "Court of Appeal" was replaced by "High Court".

3. The Equipment Interference Code of Practice

26. The Code was published on 6 February 2015. Following a consultation period it was brought into force on 14 January 2016. In the introduction the Code states:

> "1.1 This code of practice provides guidance on the use by the Intelligence Services of section 5 of the Intelligence Services Act 1994 to authorise equipment interference to which the code applies. It provides guidance on the procedures that should be followed before equipment interference can take place under that provision, and on the processing, retention, destruction and disclosure of any information obtained by means of that interference.
>
> ...
>
> 1.4 There is no power for the Secretary of State to issue codes of practice in relation to the powers and duties in section 7 of ISA. However, [the Secret Intelligence Services] SIS and GCHQ should as a matter of policy ... comply with the provisions of this code in any case where equipment interference is to be, or has been authorised pursuant to section 7 of ISA in relation to equipment located outside the British Islands.
>
> ...
>
> 7.4 If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).
>
> ..."

27. By way of footnote, the Code explains that the approach outlined in its paragraph 1.4 set out above is:

> "without prejudice as to arguments regarding the applicability of the ECHR."

28. The Code describes equipment interference as follows:

> "1.6 ... any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act [ISA], in order to do any or all of the following:
>
> (a) obtain information from the equipment in pursuit of intelligence requirements;
>
> (b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;

(c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);

(d) enable and facilitate surveillance activity by means of the equipment."

4. The Investigatory Powers Act 2016

29. The IPA became law on 29 October 2016. Some parts of the Act are already in force, it appears that others including Part 5 (see below), are to be brought into force by regulations. For a detailed overview of the IPA see *Big Brother Watch and Others v. the United Kingdom*, (nos. 58170/13, 62322/14 and 24960/15, §§ 196-202, ECHR, 13 September 2018).

30. Part 5 of the IPA concerns targeted equipment interference. It sets out provisions for issuing targeted warrants, including the requirement that they are approved by a Judicial Commissioner before being granted by the Secretary of State. The Act will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals outside the United Kingdom, even where the conduct occurs within the United Kingdom. Similarly, interference with the privacy of persons in the United Kingdom will be permitted only to the extent that it is necessary for that purpose. It will also introduce a "double-lock" for the most intrusive surveillance powers, meaning that a warrant issued by the Secretary of State will also require the approval of one of the appointed Judicial Commissioners. There will also be protections for journalistic and legally privileged material, including a requirement for judicial authorisation for the acquisition of communications data identifying journalists' sources; sanctions for the misuse of powers, including the creation of new criminal offences; and a right of appeal from the IPT on a point of law, to the Court of Appeal in England and Wales or the Court of Session (Scotland).

31. On 13 February 2017 Part 8 of the IPA providing for the appointment of the Investigatory Powers Commissioner and other Judicial Commissioners came into force. On 17 May 2018, the Commissioner announced that the Judicial Commissioners had been appointed, technical support staff recruited and that the organisation was ready to commence the new warranty regime. The Commissioner also announced that his offices are designing a new, unified inspection regime that will build on the practices developed under its three predecessors: the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner.

5. Relevant case-law

32. Following the proceedings in the IPT, the applicants sought a judicial review of the decision of the IPT insofar as it concerned section 5 of ISA. In order to do so, they argued before the domestic courts that the

"ouster" clause in section 67(8) of RIPA, which stated that decisions of the IPT should not be subject to appeal or be liable to be questioned in any court, was unconstitutional. That litigation was decided by the Supreme Court in *R (on the application of Privacy International) (Appellant) v. Investigatory Powers Tribunal and others (Respondents)* ([2019] UKSC 22) on 15 May 2019.

33. The Supreme Court found that the decisions of the IPT could be subject to challenge. Lord Carnwath for the majority reasoned that the drafter could have had no doubt that a determination vitiated by any error of law, jurisdictional or not, was to be treated as no determination at all. The reference to a determination was to be read as a reference only to a legally valid determination. The exercise was not one of ordinary statutory interpretation, as there was a common law presumption against ousting the jurisdiction of the High Court. The plain words of the subsection had to yield to the principle that such a clause would not protect a decision that was legally invalid. Therefore the exclusion in section 67(8) of RIPA applied only to determinations, awards or other decisions that were not erroneous in law.

C. Other relevant provisions

34. For a summary of a report by the European Commission for Democracy through Law (the Venice Commission) and other relevant international texts see *Szabó and Vissy v. Hungary*, no. 37138/14, §§ 21-25, 12 January 2016.

COMPLAINTS

35. The applicants complained under Articles 8 and 10 of the Convention that the power under section 7 of the Intelligence Services Act 1994 ("ISA") was not in accordance with the law in the absence of a code of practice governing its use. Moreover, they complained that that section contained no requirement for judicial authorisation; there was no information in the public domain about how it might be used to authorise Equipment Interference; and there was no requirement for filtering to exclude irrelevant material.

36. The applicants also argued under Article 13 of the Convention that the IPT had not provided an effective remedy as it had not ruled on the Section 7 regime in the domestic litigation.

THE LAW

37. Article 35 of the Convention reads as follows:

"1. The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken.

...

4. The Court shall reject any application which it considers inadmissible under this Article. It may do so at any stage of the proceedings."

A. The parties' submissions

38. The Government argued that the applicants conceded before the IPT that there was no jurisdiction under Article 1 of the Convention in respect of activities carried out under section 7 of ISA, and they conceded the argument that the section 7 regime was incompatible with the Convention. According to the Government they had not exhausted their domestic remedies as they did not raise the complaint before the IPT that the section 7 regime was unlawful because it contained no prior judicial authorisation. Finally, they underlined that the applicants had not attempted to bring a judicial review of the decision of the IPT so far as it concerned section 7.

39. The applicants argued that in their view the IPT was reluctant to rule on the question of jurisdiction without case-law guidance from Strasbourg and accordingly, they reserved their position on that point so that it could be first examined by this Court. With reference to their written pleadings before the domestic courts they argued that they did raise the point about the need for prior judicial authorisation before the IPT and that the IPT should have addressed the matter in its judgment. As to the question of judicial review, they indicated that at the time their application was lodged with this Court there was no domestic route to challenge a decision of the IPT. The judicial review of the section 5 proceedings pursued by the first applicant following the decision of the IPT represented an untried and untested procedural step, which they were not obliged to exhaust as a normal, domestic remedy.

B. The submissions of the third parties

40. In their submissions Article 19 and epic.org explained the technicalities of Equipment Interference and gave examples of its use, highlighting its nature as a powerful surveillance tool which was in their view intrusive. La Quadrature du Net, Mozilla Corporation and L.Roussey and French Data Network also explained the technicalities and uses of Equipment Interference and highlighted the importance of effective safeguards and legal oversight of such surveillance activities giving comparative examples from other jurisdictions including France. The United Nations Special Rapporteur emphasised the importance of the right to privacy and freedom of expression in the International Covenant on Civil and Political Rights and emphasised the importance of legal control over

surveillance where surveillance activities were growing in terms of their use and invasiveness.

C. The Court's assessment

41. According to the Court's well-established case law, the rationale for the exhaustion rule is to afford the national authorities, primarily the courts, the opportunity to prevent or put right the alleged violations of the Convention. It is based on the assumption, reflected in Article 13, that the domestic legal order will provide an effective remedy for violations of Convention rights. This is an important aspect of the subsidiary nature of the Convention machinery (*Selmouni v. France* [GC], no. 25803/94, § 74; *Kudła v. Poland* [GC], no. 30210/96, § 152, ECHR 2000; and *Andrášik and Others v. Slovakia* (dec.), nos. 57984/00 and 6 others). In a common law system, where the courts may extend and develop principles through case-law, it is generally incumbent on an aggrieved individual to allow the domestic courts the opportunity to develop existing rights by way of interpretation (see *Upton v. the United Kingdom* (dec.), no. 29800/04, ECHR 11 April 2006). Article 35 § 1 has a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information (see *Kennedy v. the United Kingdom*, no. 26839/05, § 110, 18 May 2010.

42. The applicants complain about Equipment Interference conducted under the power set out in section 7 of the ISA. The defining feature of that power is that it relates to acts outside the British Islands. Accordingly, the first question to be addressed in examining the compatibility of any act done under that power with the Convention is that of jurisdiction. In the context of the present case there is no doubt that addressing the question of jurisdiction called for an assessment of a number of highly complex legal and practical issues. However, the applicants appear to have conceded before the IPT that there was no jurisdiction and the IPT indicated in its "no determination" letter that it "has not been required to consider, and has not considered" the question of jurisdiction (see paragraphs 32 and 39 above).

43. Taking into account the Court's subsidiary role, the nature of the common law system, the role of the IPT and the novelty of the issue before it, the Court considers that there can be no question that the applicants needed to argue the question of jurisdiction before the IPT in order to exhaust their domestic remedies. The Court cannot accept the applicants' explanation that they did not pursue the argument about jurisdiction before the IPT in order that this Court would be able to decide the issue first (see paragraph 39 above) as this takes the opposite approach to exhaustion from that set out in Article 35, as identified in the Court's well-established

case-law and expressed in the principle of subsidiarity (see paragraph 41 above).

44. In light of its conclusion concerning the core nature of the question of jurisdiction to issues under section 7, the Court does not need to consider whether the applicants definitely invoked the specific issue of the need for prior judicial authorisation under section 7 before the IPT (see paragraphs 38-39 above).

45. The Court further notes the general arguments advanced by the applicants and also underlined in the interventions of the third parties that the surveillance complained of is particularly intrusive and that there is a need for safeguards in this domain. In that respect, the Court recalls the importance of examining compliance with the principles of Article 8 where the powers vested in the State are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated (see *Catt v. the United Kingdom*, no. 43514/15, § 114, 24 January 2019). However, that importance reinforces in the context of exhaustion of domestic remedies the need to provide the domestic courts with the possibility to rule on such matters where they have the potential to do so.

46. As to the necessity of seeking judicial review in the circumstances the Court recalls that extraordinary remedies cannot, as a general rule, be taken into account for the purposes of applying Article 35 § 1 (see *Tucka v. the United Kingdom (No. 1)* (dec.), no. 34586/10, § 15, 18 January 2011 with further references). It also considers that it was not fully clear at the time the applicants made their application to this Court that pursuing a judicial review of the IPT decision was possible. However, it cannot overlook the fact that the first applicant did attempt such proceedings, was successful and that as a result judicial review proceedings concerning the complaint under section 5 of the ISA[1] are currently pending (see paragraph 21 above). As those developments concern the same case and one of the applicants as in the present application, in the circumstances the Court does not regard that attempt at judicial review as an extraordinary remedy and concludes it was therefore a remedy to be exhausted by the applicants.

47. In these circumstances, the Court finds that the applicants did not provide the domestic courts, notably the IPT, with the opportunity which is in principle intended to be afforded to a Contracting State by Article 35 § 1 of the Convention, namely the opportunity of addressing, and thereby preventing or putting right, the particular Convention violation alleged against it.

48. In light of the foregoing, the application must be rejected as inadmissible in accordance with Article 35 §§ 1 and 4 of the Convention.

[1] Rectified on 4 September 2020: "Investigatory Powers Act 2016" was replaced by "ISA".

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 3 September 2020.

Renata Degener Deputy Registrar	Aleš Pejchal President

Appendix

1. Privacy International is an NGO registered in London and is represented by Bhatt Murphy Solicitors.

2. GreenNet Limited is an internet service provider registered in London and is represented by Bhatt Murphy Solicitors.

3. Chaos Computer Club E.V. is an association of 'hactivists' registered in Germany and is represented by Bhatt Murphy Solicitors.

4. Media Jumpstart Inc. is a company providing internet services registered in the United States and is represented by Bhatt Murphy Solicitors.

5. Riseup Networks Inc. is a company providing communications services registered in the United States and is represented by Bhatt Murphy Solicitors.

6. Korean Progressive Network Jinbonet is an internet provider registered in South Korea and is represented by Bhatt Murphy Solicitors.