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

Communicated on 19 November 2018

FIRST SECTION

Application no. 46259/16
Privacy International and Others
against the United Kingdom
(see list appended)

STATEMENT OF FACTS

A list of the applicants is set out in the Appendix.

The facts of the case may be summarised as follows.

A. Background circumstances

1. 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.

2. 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 21 below).

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

> "...
>
> 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.
>
> ..."

4. 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.

The Investigatory Powers Tribunal

5. 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.

6. 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."

7. 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. However, during 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 paragraph 22 below).

8. 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"), were rendered lawful where a warrant or authorisation to conduct Equipment Interference had been obtained under sections 5 or 7 of the ISA, respectively.

9. 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.

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

11. 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."

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.

12. 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 was 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.

13. 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."

14. 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 paragraph 24 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."

15. 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 section 7 but that in any event the answer concerning jurisdiction for section 5 would be the same as for section 7, that is to say ordinarily there would be no jurisdiction (see paragraph 12). 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.

16. The IPT concluded:

> "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."

17. 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."

B. Relevant domestic law and practice

1. The Computer Misuse Act 1990

18. 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.

19. 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 below) does not commit an offence.

2. The Intelligence Services Act 1994

20. 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."

21. 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."

3. The Equipment Interference Code of Practice

22. 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).

..."

23. 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."

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

24. 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).

25. 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 new protections for journalistic and legally privileged material, including a requirement for judicial authorisation for the acquisition of communications data identifying journalists' sources; tough 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).

26. 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. The Intelligence Services Commissioner

27. The Office of the Intelligence Services Commissioner was created under statute. The Commissioner's primary role was to ensure that the United Kingdom intelligence agencies and parts of the Ministry of Defence lawfully and appropriately use the intrusive powers available to them. The Commissioner's oversight was in part conducted by checking warrants and authorisations issued by Secretaries of State and the internal authorisations that enable the Intelligence Agencies to carry out their functions, checking that proper consideration has been given to necessity, proportionality and reasonableness.

28. The Office of the Intelligence Services Commissioner was replaced on 1 September 2017 by the Investigatory Powers Commissioner's Office, a body created under the IPA (see section 4 above). In part v. of his Annual Report for 2014, the Intelligence Services Commissioner explained the use of Section 7 authorisations as follows:

> "Under Section 7 of ISA the Secretary of State (normally the Foreign Secretary) may authorise activity outside of the United Kingdom necessary for the agencies to properly discharge one of their functions. Authorisations may be for a particular operation or may be related to a broader class of operations [class authorisations].
>
> ...
>
> Class authorisations cover the essential and routine business of SIS and GCHQ. Again, they fulfil two functions. First they give protection for liability under UK law and second they provide political approval for activities authorised by the class authorisation."

29. In his Annual report for 2016, in part iii. he comments:

> "This area of activity [equipment interference] is currently authorised under the authority of ISA section 5 warrants or section 7 authorisations but will fall under the IPA Part 5 in the future.
>
> ...

In my 2015 report I outlined the oversight process for EI, including how I work with the agencies to provide oversight and I explained that particular consideration is given where an operation is likely to obtain confidential personal information, confidential journalistic material, communications subject to legal privilege or communications between an MP and another person on constituency business. I highlighted that the current interference does not provide for bulk EI authorisations other than under section 7. Part 6 Chapter 3 of the IP Act sets out new powers to obtain bulk EI warrants. It is vital that any authorisations made in this area set out full consideration of necessity and proportionality principles, and maintain appropriate handling of confidential data.

My overall assessment

The EI code under RIPA was finalised in January 2016. That code made public the powers and safeguards that existed previously. I believe that changes brought in under the Investigatory Powers Act will provide greater clarity. I have been pleased to see that the agencies are proactively engaging with recommendations I have made in the past and taking steps to improve compliance with the Code of Practice. In general, I am satisfied that necessity and proportionality considerations are carefully considered, and that the case for intrusion into privacy is made clear to the authorising officer in relation to EI authorisations."

C. Other relevant provisions

30. 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

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

32. The applicants also argued under Article 13 that the IPT did not provide an effective remedy as it did not rule on the Section 7 regime in the domestic litigation.

QUESTIONS TO THE PARTIES

1. Can the applicants claim to be victims of a violation of the Convention, within the meaning of Article 34 in particular in light of *Roman Zakharov v. Russia* [GC], no. 47143/06, §§ 170-172, ECHR 2015?

2. Have the applicants exhausted all effective domestic remedies, as required by Article 35 § 1 of the Convention?

In particular, in light of the "no determination" letter from the Investigatory Powers Tribunal did the applicants invoke before the national authorities at least in substance, the question of the jurisdiction of the United Kingdom?

Did the applicants invoke before the national authorities, at least in substance, the rights under Article 13 on which they now wish to rely before the Court?

3. Did the facts of which the applicants complain in the present case occur within the jurisdiction of the United Kingdom?

4. Has there been an interference with the applicants' right to respect for their private life, within the meaning of Article 8 § 1 of the Convention?

If so, was that interference in accordance with the law and necessary in terms of Article 8 § 2?

5. Has there been an interference with the applicants' freedom of expression, within the meaning of Article 10 § 1 of the Convention?

If so, was that interference prescribed by law and necessary in terms of Article 10 § 2?

6. Did the applicants have at their disposal an effective domestic remedy for her Convention complaints, as required by Article 13 of the Convention?

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.