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 COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT 14/120-126/CH**
BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, 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 COMMUNICATION HEADQUARTERS

Defendants

CLAIMANTS' REPLY

---

1. Save where expressly admitted, the assertions of fact and law in the Open Response are denied.

2. References to paragraph numbers are to the numbered paragraphs of the Open Response.

3. As to paragraphs 4-9:

    a. The Agencies' 'NCND' policy is noted and may be an appropriate means of protecting the public interest in some cases. Nevertheless, it is a government policy, not a rule of law applicable in the IPT. It requires justification in each case, and represents a significant departure from principles of open justice

and disclosure. Nor is it applicable in all circumstances. See Maurice Kay LJ in *CF* [2014] EWCA Civ 559.

b. In particular, the existence of widely-used operational methods and techniques that are openly used by other nation states (and non-state actors) makes much of the NCND case pleaded in the Open Response unsustainable. The Claimants plead to this in more detail below.

4. As to paragraph 13, the IPT's open jurisdiction is wider than considering pure issues of law. It has previously heard entire cases, including issues of fact, on an open, *inter partes,* basis. It also has power to hear argument on open issues of fact or law, and to order disclosure where to do so would not harm the public interest.

5. Paragraph 19 is denied and contains an over-broad claim as to the content of the Closed Response. In order to determine this issue, the Tribunal is invited to appoint a Special Advocate to represent the interests of the Claimants.

6. As to paragraph 21, until the Open Response was served, the position of the Agencies was that it neither confirmed nor denied whether it even carried out CNE operations. In those circumstances, CNE was not prescribed by law because there was no accessible framework under which it was (even in general terms) admitted or governed. *All* of the relevant rules and guidance were secret.

7. The Respondents have now sought to resile from their admission in their Response to the Request for Further Information about paragraph 21. The Response asserts "*the Respondents can neither confirm nor deny whether public authorities (generally so defined) have, in fact carried out such* [CNE] *operations*". This is an over-broad, unjustified and false claim to rely on the 'NCND' policy.

8. The Response was served on 20 March 2015. 8 days previously, on 12 March 2015, the ISC published its report "*Privacy and Security*". In its report, the ISC said:

IT OPERATIONS: CNE ***

GCHQ conduct IT Operations[181] both within the UK and overseas. During 2013 a significant number (around ***%) of GCHQ's intelligence reports contained information that derived from IT Operations against a target's computer or network[182] – GCHQ call this 'Computer Network Exploitation' (CNE). GCHQ undertook the following CNE operations during 2013:

- ***;[183]
- ***; and
- ***.

In addition to CNE operations to obtain intelligence, ***:

- ***;
- ***; and
- ***.[184]

---

[181] *The draft 'Equipment Interference Code of Practice' (6 February 2015) sets out the safeguards that the Agencies must apply in relation to the handling, processing, retention, disclosure and destruction of any information obtained through IT Operations. This includes particular controls for communications that involve legally privileged material, confidential personal information, journalistic material or communications between MPs and their constituents.*

[182] *Oral Evidence – GCHQ, 26 June 2014.*

[183] *This included *** 'persistent' operations (where the implant 'resides' on an SoI's computer for an extended period) and *** non-persistent operations (where the implant expires when the user's internet session ends).*

[184] *Written Evidence – GCHQ, 14 November 2014.*

9. See also paragraph 173 of the ISC report ("*IT Operations undertaken by the Agencies include operations against… a specific device… a computer network*"), paragraph 178 ("*GCHQ undertook *** operations under section 7 of ISA authorising them to interfere with computers *** overseas*") and footnote 179 ("*These operations vary considerably in both scale and impact*").

10. It is therefore an improper and over-broad national security claim to suggest that the Respondents cannot confirm or deny the fact of CNE and considerable detail about CNE operations in circumstances when the ISC has published reports setting out considerable detail and confirming that:

    a. Such operations are carried out by GCHQ both within the UK and overseas.

b. In 2013, a significant number of GCHQ's intelligence reports contained information that derived from CNE operations.

c. The phrase "*CNE operations*" is itself a term of art used by GCHQ.

d. Specific examples of CNE operations were given to the ISC.

e. The types of operation include "*persistent*" operations involving an implant residing on the subject's computer for an extended period and "*non-persistent*" operations where the implant expires at the end of an internet session.

f. GCHQ's CNE operations vary considerably in scope and impact.

11. Paragraph 45 is denied. Where Crown servants abroad carry out CNE, the relevant offence is deemed to have taken place in the UK. See section 31 of the Criminal Justice Act 1948.

12. Paragraph 64 is denied. S. 5 warrants and s. 7 authorisations do not, of themselves, provide a sufficient legal framework for the purpose of Article 8 ECHR, nor do they have the effect of removing civil or criminal liability for interferences under section 3 of the CMA.

13. Paragraph 66 is denied. The draft Code does not "*fully reflect… the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by GCHQ*". The Claimants will seek disclosure, subject to any legitimate public interest concerns. Prior to disclosure, the Claimants rely on:

a. the disclosure given in *Belhaj* which confirms that GCHQ has not always applied the safeguards in the draft Code to privileged material; and

b. the admission to this effect in paragraph 9 of the Response to the Request for Further Information ("*the safeguards at paragraph 3.18 were not previously part of GCHQ's practice or policy*").

14. As to paragraph 71, the draft EI Code fails to properly reflect the effect of ss. 3 and 10 of the CMA, and does not remove civil or criminal liability for certain types of computer misuse. The Claimants note that the Defendants have, despite a request for

Further Information (of Footnote 17), failed to plead to the effect of ss. 3 and 10 of the CMA as a matter of law or to paragraphs 36 and 37 of the Grounds. An appropriate application will be made in due course.

15. As to paragraphs 94-98, the authorisation of highly intrusive surveillance activity in an individual case under a s. 7 class authorisation does not require the approval of the Secretary of State. Such arrangements are inadequate to protect against arbitrary conduct. Further, the ISC report disclosed that the Respondents do not keep detailed records of operational activity carried out under class authorisations issued under s. 7 ISA (ISC recommendation BB). GCHQ apparently has 5 such authorisations, and their scope includes "*interference with computers*" (ISC Report, paragraph 234). Such failures are not compatible with the "prescribed by law" requirement in Article 8. Unless proper and detailed records are kept, the Commissioner has no prospect of being able to investigate unjustified or excessive conduct, and there will be no documentary evidence of such intrusive activity for the IPT to review if and when a claim is brought.

16. As to paragraph 101, the Property Code is not a sufficient basis on which to assert that CNE activity is prescribed by law. It fails to put in place any of the special procedures required for such conduct, hence why a draft Code has now been prepared and published. Indeed, the Property Code does not make any reference to CNE at all. It therefore provides no proper, and certainly no accessible, guidance or information as to the circumstances in which interference will occur.

17. As to paragraph 125, it is denied that a Commissioner is or has been an effective mechanism to ensure that there are sufficient, lawful and adequate safeguards in place to protect people who may be subject to CNE. Further, it appears that the Commissioner has only seen the "*main arrangements*" and the date of his review has not been disclosed, a request for that date having been ignored (Response to Request for Further Information, paragraph 23).

18. As to paragraph 130, Sir Malcolm Rifkind resigned as Chairman of the ISC following allegations that he was prepared to accept work from reporters purporting to be from a Chinese company. Sir Malcolm denied wrongdoing, but accepted that he "*may have made errors of judgment*". The ISC have not elected a new Chair and do not intend to do so before the General Election.

19. As to the proposed issues, the Claimants agree in part and disagree in part with the proposed formulation. As in other recent cases before the IPT, the Claimants propose that they should exchange drafts with the Respondents and seek to agree a draft order for approval by the Tribunal at the directions hearing listed for 1 May 2015.

20. As to paragraph 155, the Claimants reserve their position on the correctness of the IPT's analysis in *Liberty/Privacy International*. Safeguards which operate in secret are not sufficient to provide proper protection against arbitrary conduct. In any event, that analysis has no applicability where all or essentially all of the relevant safeguards are secret, rather than simply "*the precise details*" of those safeguards.

BEN JAFFEY

TOM CLEAVER

BHATT MURPHY

1 April 2015