Privacy International and Greennet & Others v The Secretary of State for Foreign and Commonwealth Affairs and The Government Communications Headquarters ("GCHQ") [2016] UKIP Trib 14_85-CH

Jack Williams, Pupil Barrister

1 March 2016

Following revelations by American whistleblower Edward Snowden (the former NSA employee and CIA contractor) regarding the extent of surveillance carried out by national authorities, Privacy International and seven Internet Service Providers ("ISPs") launched a legal challenge against GCHQ's alleged use of Computer Network Exploitation ("CNE") and so-called "thematic" warrants under the Intelligence Services Act 1994 ("the ISA 1994").

CNE (commonly known as "hacking") includes the capacity to obtain information from a particular device, server or network, and create, modify or delete information on any such device, server or network. It has been suggested that CNE may even include the capacity to activate microphones and cameras on devices remotely without the owner's permission or knowledge.

Thematic warrants do not identify targeted individuals or addresses but rely on general categorises of people or places so that, for example, GCHQ can target an entire class of property or persons such as "all phones in Birmingham".

The Claimants alleged that both practices were unlawful.

The Investigatory Powers Tribunal ("the IPT" or "the Tribunal") heard the case at the end of 2015, giving judgment on 12 February 2016. The Tribunal was ultimately satisfied that with GCHQ's new Equipment Interference Code of Practice ("the EI Code"), and whatever the outcome of Parliamentary consideration of the Investigatory Powers Bill, a proper balance is being struck between, on the one hand, the need of the Intelligence Agencies to safeguard the public and, on the other hand, the protection of individuals' rights to privacy and freedom of expression. The Tribunal therefore ruled that CNE and so-called thematic warrants are legal and do not infringe upon individuals' rights contained in Articles 8 and 10 of the European Convention on Human Rights.

The judgment is available here. References in square brackets below refer to paragraph numbers in this judgment.

Factual background

Given the sensitivity of the issues with which it is dealing and a desire to provide open judgment, the IPT proceeded (as it has done before) on the basis of assumptions as to the facts with a view to reaching legal conclusions on that basis. It can then separately consider specific factual positions thereafter in closed session if the Respondent's assumed conduct is found to be unlawful ([2]). In open session the Respondents will often maintain the well-known policy that they "neither confirm nor deny" ("NCND") any particular factual matters such as the existence of specific operations. However, for the first time in a court case, GCHQ admitted that:

(a) it carries out CNE "within and outside the UK" (though it was not admitted that CNE was carried out prior to February 2015);

(b) it undertakes "persistent" (where implants are left implanted on a targeted device) as well as "non-persistent" (where monitoring ends with each internet session) operations;

(c) in 2013, about 20 per cent of its intelligent reports contained information derived from CNE;

(d) CNE operations undertaken by GCHQ can be against a specific device or a computer network; and

(e) it has obtained warrants under both sections 5 and 7 of the ISA 1994 ([5]).

Legal background

The powers and functions of GCHQ are set out in Section 3 of the ISA 1994.

Section 5 of the ISA 1994 requires GCHQ to apply to the Secretary of State for a warrant to enter or interfere with property or wireless telegraphy. The Secretary of State may issue a warrant (a "section 5 warrant") authorising the taking of such action "*as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified*" if, *inter alia*, the Secretary of State "*thinks it is necessary for action to be taken*" to assist GCHQ in its functions, "*is satisfied that the taking of the action is proportionate to what the action seeks to achieve*", and "*is satisfied that satisfactory arrangements*

are in force" regarding disclosure of information.

Section 7 of the ISA 1994 contains similar provisions to those in Section 5 for the authorisation of acts outside the British Islands (a "section 7 authorisation").

Section 3 of the Computer Misuse Act 1990 ("the CMA 1990") creates an offence for unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of computers.

After its amendment in May 2015 (pursuant to the Serious Crime Act 2015), Section 10 of the CMA 1990 expressly makes it clear that a person acting under a section 5 warrant or a section 7 authorisation does not commit an offence under section 3 of the CMA 1990.

Judgment

In a lengthy judgment, a range of issues (as agreed by the parties) was addressed by the Tribunal. Each will be dealt with in turn with the exception of issues 2 (territorial jurisdiction of sections 5 and 7 ISA 1994), 5 (scope of the European Convention on Human Rights), 7 (the absence of a similar certificate to that in section 16 RIPA) and 10 (legal professional privilege) which, for various reasons, were only dealt with summarily, were immaterial, and/or were reserved for appropriate future cases.[1]

Was an act which would be an offence under section 3 of the Computer Misuse Act 1990 made lawful by a section 5 warrant or section 7 authorisation prior to the amendment of section 10 of the Computer Misuse Act 1990 as of May 2015?

The Claimant submitted that until the passage of the amendment to section 10 of the CMA 1990, any act of CNE which would contravene section 3 of the CMA 1990 was unlawful. On the Claimants' case, the amendment to the section was necessary in order to reverse the position ([16]) because the express savings clause in the unamended CMA 1990 (*"Section 1(1) above has effect without prejudice to the operation … of any enactment relating to powers of inspection, search or seizure…")* does not mention section 3 and additionally could not be impliedly overruled by the subsequent ISA 1994 ([17]).

The Tribunal dismissed these arguments, holding that the wording in section 10 of the CMA 1990 (as unamended) *"had no effect upon and/or was expressly overtaken by the clear words of ss.5 and 7 of the ISA"* ([20]). Indeed, the IPT considered that it would be *"extraordinary"* if steps taken under the express powers of sections 5 and 7 of the ISA 1994 *"could be rendered unlawful by*

[1] See [23], [53], [63] and [88] respectively.

reference to a saving under an earlier statute" especially where the language of sections 5 and 7 contain "*an express removal of civil or criminal liability*" ([20]). The amendment to the CMA 1990 in May 2015 was deemed "*simply clarifactory*" ([20]).

Does the power under section 5 of the ISA 1994 to authorise interference with "property" encompass physical property only, or does it also extend to intangible legal rights?

The IPT noted that the Claimants' submissions in this matter (alleging that "property" only referred to physical property) seemed "*to evaporate in the course of argument*" ([27]). Accordingly, only short attention was given to the matter. Noting that there is no definition of the word "property" in section 5 itself, the Tribunal commented that there was "*no justification whatever*" for a narrow construction of the phrase ([28]), and went on to agree with the view of the Intelligence Services Commissioner in his report of June 2015 that section 5 of the ISA 1994 extends to intangible property whether the action is directed at intangible property alone or is ancillary to interference with physical property ([28]).

Thematic warrants – what is the meaning of the words "in respect of any property so specified" for the purposes of the issue of a section 5 warrant?

Despite taking issue with the commonly-used title "thematic warrants" (at [31]), the Tribunal went on to consider the Claimants' submission that such general warrants (which do not identify targeted individuals or addresses but rely on general categorises of people or places) are unlawful.

The Claimants relied on four arguments to support their interpretation of the phrase "property so specified" in section 5 as requiring the identification of the property/equipment at the date of the warrant ([35]): first, common law cases such as *Entick v Carrington* [1765] 2 Wilson KB 275 exclude general warrants; second, the wording of section 5 is in contrast to that in section 7 (the latter including the words "acts" and "in the course of an operation"); third, identification cannot, or should not, depend upon the belief, suspicion, or judgment of the officer acting under a warrant; and fourth, passages in Hansard relating to the new Investigatory Powers Bill might suggest a narrower interpretation.

The Respondents, in turn, submitted that ([36]): first, the common law cases relate to limitations on executive acts, whereas section 5 is a creature of statute, is in a different context of national security, and includes built-in limitations of legality, necessity, and proportionality; second, section 7 is a different provision and is not in direct contrast to, or an alternative to, section 5; third, it is not

necessary to identify persons any more than is possible at the time of the issue of the warrant, and it is not necessary for individuals to be identified by name or by reference to the particular time when the warrant is issued – all that is required is that there is as much information as possible for the Secretary of State to fulfil his obligations to assess the legality, necessity and proportionality of the warrant; and fourth, the Investigatory Powers Bill brings together powers already available and is consistent with section 5.

Ultimately the IPT agreed with the Respondent in reaching the conclusion that a section 5 warrant:

> *"is lawful if it is as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those exercising the warrant, so that the property to be covered is objectively ascertainable, and it need not be defined by reference to named or identified individuals" ([89(iv)] and see [38] and [47]).*

Accordingly, the word "specified", in the IPT's view, "*cannot have meant anything more restrictive*" than "adequately described" ([44]). It held so for five reasons: first, with regards to the common law cases cited by the Claimants, the Tribunal considered them "*not in our judgment a useful or permissible aid to construction of an express statutory power*" for the reasons submitted on behalf of the Respondents ([37]); second, other statutes using the word "specified" do not require particular property to be provided, but instead simply require *specification* of the property which, in turn, requires *sufficiency of identification* rather than particular property ([39]); third, once the issue becomes seen as one of sufficiency rather than particularity, any disagreement over the sufficiency of any specification is subject to the scrutiny by the Intelligence Services Commissioner, by the ISC and by the IPT itself ([38]); fourth, the Property Code (at 7.18-7.19) and the new EI Code (at 4.6) include lengthy lists of what is required to be included in an application to the Secretary of State thus reducing any risk of insufficiency of identification ([40]); and fifth, the IPT considered that the Claimants' submissions "*confused the property to be specified with the person or persons whose ownership or use of the equipment may assist in its identification*" ([41]).

Does a section 5 warrant satisfy the criteria (1) – (3) of the Weber?

The Claimant submitted, relying on *Malone v UK* [1985] 7 EHRR 14 [2] and *Weber and Saravia v Germany* [2008] 46 EHRR SE5, that if the wider interpretation of "property so specified" were adopted by the Tribunal (as it was), then a warrant so issued would not be in adequate compliance with the Convention for reasons of overly-wide discretion.

[2] See para. 67 in that case

The European Court of Human Rights set out the so-called '*Weber* criteria', as numbered (1) – (6) by the IPT in *Liberty/Privacy (No. 1)* [2015] 3 AER 142 at paragraph 33, as follows:

> *"In its case-law on secret measures of surveillance, the Corut has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed."*

The Claimants' argument was rejected by the Tribunal. In applying *Weber* criteria (1) – (3), the Tribunal noted that in *Weber* itself "*a far broader and less specified warrant than the s.5 warrant*" was found to comply with the Convention ([58]). The IPT held that a warrant which specifies the property proposed to be covered by it as to enable a Secretary of State to be satisfied as to its legality, necessity and proportionality (so that the property covered is objectively ascertainable, regardless of the fact that it is not defined by reference to named or identified individuals) *does comply with* (1) – (2) of the *Weber* criteria and so Articles 8 and 10 ECHR ([59]). A warrant issued under section 5 of the ISA 1994 lasts for six months unless renewed for a further six months (section 6 of the ISA 1994), thus satisfying (3) of the *Weber* criteria ([57]).

Post-February 2015, does a section 5 warrant satisfy the criteria of (4) – (6) of Weber?

During the proceedings (on 6 February 2015), the Respondent published the EI Code pursuant to section 71 of the Regulation of Investigatory Powers Act 2000. This was laid before Parliament in November 2015, and, since the hearing, has been brought into force (14 January 2016). GCHQ accepted that it had been bound as a matter of public law by the EI Code since February 2015. Prior to such publication of the EI Code, the Respondent's safeguarding procedures were to be found in the Covert and Surveillance and Property Inference Code ("the Property Code").

In order to evaluate whether section 5 warrants are and were compliant with (4) – (6) of *Weber* criteria (quoted above), the Tribunal therefore had to evaluate two separate timeframes: post February 2015 (the EI Code) and prior to February 2015 (the Property Code). The Tribunal dealt with the EI Code first.

The Tribunal began (at [65]) by repeating a paragraph from its judgment in

Liberty/Privacy (No. 1) in which it summarised the requirements from ECHR *Weber*-line of jurisprudence: *"It is in our judgment sufficient that: i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted such as to give an adequate indication of it… ii) They are subject to proper oversight."* Put simply, there has to be adequate safeguards for the protection of the product of CNE and a satisfactory system of oversight for the scheme to be held up as compliant with the ECHR (see, also, [74]).

In this regard, the Tribunal noted that the *"significant paragraphs of the EI Code relating to Weber (4) to (6) are in Sections 5 and 6"* ([68]). These paragraphs set out the "keeping of records" (para. 5) for warrants which are "centrally retrievable for at least three years" (para. 5.1) and the "handling of information and safeguards" (para. 6) including policies as to "use of information (para. 6.3), "handling information" (para. 6.4 – 6.5), "dissemination of information" (para. 6.6 – 6.7), "copying" (para. 6.8), "storage" (para. 6.9), and "destruction" (para 6.10).

Materially, the IPT held (at [70]):

> *"We have no doubt at all that, insofar as compliance must be shown with Weber (4) to (6), the EI Code does so comply, and has so complied since its publication in 6 February 2015… We are satisfied that the requirements for records are sufficient and satisfactory, and that adequate safeguards have been in place at all times for the protection of the product of CNE, and that there exists a satisfactory system of oversight."*

The Tribunal accordingly found that a proper balance is being struck between, on the one hand, the need of the Intelligence Agencies to safeguard the public and, on the other hand, the protection of individuals' rights to privacy and freedom of expression ([90]). Against the fact that CNE inevitably goes beyond interception as it accesses what is not, and would not be, communicated ([3]), the Tribunal weighed: (i) difficulties for the Intelligence Agencies caused by the *"increasing use of encryption"* by suspects ([3]); (ii) the currently *"severe"* security situation in the United Kingdom ([3]); (iii) the fact that *"technological capabilities… lie at the very heart of the attempts of the State to safeguard the citizen against terrorist attack [sic]"* ([3]); (iv) the safeguards of the Intelligence Services Commissioner ([65]); (v) the safeguarding procedures in the EI Code ([68]); and (vi) the fact that it is an offence for a member of the Security and Intelligence Services to disclose information without lawful authority or retain it without lawful authority (sections 1 and 8 respectively of the Official Secrets Act 1989, and see, also, section 19 of the Counter-Terrorism Act 2008 and the fifth and seventh data protection principles of the Data Protection Act 1998).

Prior to February 2015, did a section 5 warrant satisfy the criteria of (4) – (6) of Weber?

This, the Tribunal confessed, was the *"more difficult question"* (at [72]). By definition, if the publication of the EI Code in February 2015 improved the position, and made sufficiently public the arrangements which govern the use by the Respondents of their powers, the arrangements prior to that date (the Property Code) must have been inferior.

Despite it being more difficult, the IPT reached the same conclusion as it did regarding the period post February 2015, namely that the scheme was ECHR-compliant.

A particular difficulty for the Tribunal was *R.E. v United Kingdom* (Application No. 62498/11, 27 October 2015) in which the ECtHR addressed the Property Code by contrasting it with the Interception of Communications Code of Practice which the ECtHR had approved in *Kennedy v United Kingdom* (2011) 52 EHRR 4. *RE* concerned the issue of safeguarding legally and professionally privileged communications in relation to covert surveillance. The Strasbourg Court held, in that context, that (4) – (6) of the *Weber* criteria were *not* satisfied by the Property Code.

The Tribunal sought to distinguish this case (at [80]) on the grounds that in *RE,* the ECtHR:

> *"was addressing a specific and different question, the matter of adequate protection for LPP communications in respect of covert surveillance" ([79]). Therefore, the Tribunal reasoned, "[w]hen the ECtHR addressed… the benefits of the Interception Code, it is plain to us that they were doing so not in respect of Weber (4) to (6) generally, but in respect of the way in which the Interception Code gave improved safeguards by protecting "the interests of persons affected by the surveillance of legal consultations". The Court did not address specifically, and reach conclusions as to, whether the Property Code was inadequate (other than in respect of LPP) to comply with the Weber (4) to (6)."*

Specifically, the Tribunal analysed paragraphs 4 (oversight by Director of GCHQ), 8.3 (retention of records), and 9.3 (arrangements for secure handling, storing, access, sharing, and destruction of information), of the Property Code. It held that it was *"satisfied that* [these] *would be adequate, in the context of the interests of national security, to impose the necessary discipline on GCHQ and give adequate protection against arbitrary power"* ([77]). Additionally, the Tribunal had regard to the statutory obligations of and upon GCHQ (referred to above) which are more significant than those imposed upon the police, the

additional 'under the waterline arrangements' which were signposted, and the oversight by the Intelligence Services Commissioner of GCHQ's compliance with their obligations ([80]).

The Tribunal therefore concluded that *"[i]f there was inadequacy within the Property Code, as compared with the EIC, we do not conclude that the inadequacy was in the circumstances such as to constitute a contravention of Articles 8/10"* ([82]).

Additional Comment

This case, in the words of the Tribunal itself, *"obviously raised a number of serious questions"* ([90]). It is the latest in a line of cases (*Malone* (ECtHR), *Weber* (ECtHR), *Liberty* (ECtHR), *Kennedy* (ECtHR), *Liberty* (IPT), *Belhadj* (IPT) *inter alia*) which each address the various powers and extent of surveillance by security agencies. The case highlights, once again, the significant hurdles that any claimant will have to jump over in order to challenge state activity in this (legally-complex) area. It is expected that the judgment will put into sharp focus the extent of GCHQ's surveillance capabilities and the significant implications for the rule of law and the separation of powers.

The case is significant for a number of other reasons. First, it was the first time in which GCHQ admitted to carrying out various surveillance activities in the UK and overseas; this openness is at least a small, but welcome, development for public oversight. Secondly, a number of positive 'by-products' arose as a result of the proceedings: the publication of the EI code, the signposting of more 'below the waterline' arrangements previously unknown, and the amendment of the CMA 1990 by the Serious Crime Act 2015.

There is, of course, no right of appeal to any higher UK court from an IPT judgment. It remains to be seen whether Privacy International or any of the ISPs challenge the decision in Strasbourg, as entitled, and what effect any challenge (or lack of) will have on the passage of the Investigatory Powers Bill through Parliament.

Daniel Beard QC was instructed for the Respondents.

The comments made in this case note are wholly personal and do not reflect the views of any other members of Monckton Chambers, its tenants or clients.

Monckton Chambers
1 & 2 Raymond Buildings
Gray's Inn
London, WC1R 5NR

Tel: +44 (0)20 7405 7211
Fax: +44 (0)20 7405 2084
Email:chambers@monckton.com
www.monckton.com