Case No. IPT 14/85/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

Case No. IPT 14/120-126/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

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

Claimants

and

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

Respondents

INDEX OF OPEN EXHIBITS TO RE-RE-AMENDED OPEN RESPONSE

Exhibit No	Description
1	**Compliance Guide – Authorisations**
2	**ISA Section 5 guidance**
3	**ISA Section 7 guidance**
4	**Extract from current Advanced Training for Active Operations**
5	**Summary of differences between current and past versions of Section 5 and 7 Guidance**

[Exhibit 1]

The underlined parts of this document indicate that it has been gisted for OPEN

Compliance Guide – Authorisations

Scope

This section describes the legal authorisation that GCHQ uses to ensure that it conducts collection and targeting lawfully. It also describes the policy authorisations that you are required to obtain before carrying out certain sensitive or specialist forms of targeting or analysis. It provides details of the processes you must follow to obtain these authorisations.

Interference with property and wireless telegraphy; removing liability for other actions overseas

The ISA warrant and authorisations scheme is a mechanism for removing liability that would otherwise attach to interference with property such as computers, phones and routers. This interference would otherwise be a criminal offence under the Computer Misuse Act. ISA authorisations may also remove liability that would otherwise attach under other UK laws such as the Terrorism Act 2006 or the Communications Act in relation to GCHQ activities overseas. GCHQ uses these authorisations to cover CNE. If you are unsure whether you require an ISA warrant or authorisation, please contact the relevant personnel.

1. Actions Overseas (ISA Section 7)

An ISA s.7 authorisation approved by the Secretary of State is the legal instrument that removes criminal liability in the UK for GCHQ actions overseas which might otherwise be an offence in UK law. Such an authorisation is also capable of removing any civil liability in the UK that might arise as a result of GCHQ's actions overseas. An ISA s.7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations. Wherever possible, GCHQ seeks to rely on class authorisations, including a class authorisation which permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant).

2. Actions having effect in the UK (ISA Section 5)

An ISA s5 warrant authorises interference in the UK with property, equipment or wireless telegraphy. It may be issued on grounds of National Security or the Economic Well-Being of the UK.

A Secretary of State must normally approve a new ISA s5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its issue, but only subject to particular rules. You should consult the relevant personnel for advice.

[Exhibit 2]

The underlined parts of this document indicate that it has been gisted for OPEN

Updated: January 2015

ISA Section 5 guidance

ISA warrants

Warrants issued under the Intelligence Services Act (ISA) authorise interference with property (eg equipment such as computers, servers, routers, laptops, mobile phones, software, intellectual property etc), or wireless telegraphy.

A **section 5 warrant** authorises interference with property or wireless telegraphy in the British Islands. It may only be issued on grounds of National Security or the Economic Well-Being of the UK. A section 5 warrant is signed by a Secretary of State and is valid for 6 months from the date of signature, at which point the warrant should be renewed or cancelled.[1]

The relevant personnel are responsible for preparing warrant submissions, based on the business case provided by the analyst completing the request form and with input from GCHQ's legal team. Submissions are then reviewed by GCHQ's Legal Advisers and approved by a GCHQ official of appropriate seniority, before being sent to the relevant Department for signing.

Warrant submissions are read by a Secretary of State and senior government officials. They may also be selected by the Intelligence Services Commissioner during one of his twice-yearly inspections. The business case therefore needs to be easily understood by a non-technical reader, should avoid technical jargon and be written to a good standard of English. It should be clear and concise, but include sufficient detail about the proposed operation that the Secretary of State is fully aware of what he is authorising.

Requesting a new Section 5

Requests for new warrants and renewals must be sponsored by an appropriately senior official, who must be satisfied that the proposed operation is justified, proportionate and necessary.

Part I. – to be completed by the relevant GCHQ team

The intelligence case should be fit for purpose for signing by a Secretary of State, avoiding unnecessary jargon and technical terminology. The case should include:

- the intelligence background;
- the priority of the target within the priorities framework as endorsed by JIC and NSC;

[1] The underlined words in this quotation are in the original.

- an explanation of why the proposed operation is necessary;
- a description of any other agency involvement in working the target;
- the intelligence outcome(s) the proposed operation is expected to produce.

As CNE techniques are by nature intrusive, an explanation of how proportionality will be maintained should be given. Key points to consider include:

- the expected degree of invasion of a target's privacy and whether any personal or private information will be obtained;
- the likelihood of collateral intrusion, ie invading the privacy of those who are not targets of the operation, eg family members;
- whether the level of intrusion is proportionate to the expected intelligence benefit;
- a description of the measures to be taken to ensure proportionality.

An assessment of the political risk also needs to be included.

The form is then returned to the sponsor to consider whether, in light of the CNE input, they can recommend to the Secretary of State that the operation is justified, proportionate and necessary, and that they are aware of the risk. If so, they should sign and date the form and send it to the relevant personnel.

The Section 5 Guidance also explains that the process is completed by the preparation of a formal submission and a warrant instrument. These are reviewed by GCHQ Legal Advisers and the sponsor, then sent for signature to the relevant Department, which will follow its own internal procedures before the documents are passed to the Secretary of State for consideration. Once the warrant has been signed, relevant personnel will be informed that the operation can go ahead.

Section 5 renewal process

A reasonable period before a warrant is due to expire, the relevant personnel will request a case for renewal from the relevant personnel, copying the sponsor and include a copy of the previous submission. The analyst should confirm with the sponsor that renewal is required, and if so, provide the relevant personnel with a business case by the specified deadline. This should include:

- an update of the intelligence background, ensuring it accurately reflects the current context of the warrant;
- details of any developments and intelligence gained since the warrant was issued/last renewed – this **must** address any expectations highlighted in the previous submissions;

- a review of the level of intrusion, based on the evidence of the activity authorised by the warrant;
- a review and, if necessary, update of the political aspects of the risk assessment;

The relevant team should provide the following information:

- any updates on technical progress made since the warrant was last renewed
- an updated operational plan – again, this **must** address specific actions or plans laid out in the previous submission
- any updates to the risk assessment.

Again, the relevant personnel may need to work with the originator and the relevant team to strengthen the renewal case, and will also consult the Legal Advisers before providing a copy to the sponsor for final review. When the sponsor is content that the submission is accurate and demonstrates that the operation is still justified, necessary and proportionate, the relevant personnel will submit the renewal application to the relevant Department for signature.

If a warrant is no longer required, it should be cancelled. If not renewed or cancelled, the warrant will expire on the date specified and the activity will no longer be authorised.

It is good practice to cancel warrants as soon as the requirement for the operation has ceased.[2]

Section 5 cancellation process

When a warrant is no longer required, the analyst should send the relevant personnel a short explanation of the reason for the cancellation. When the team conducting the operation confirms that the operation is fully drawn down, the relevant personnel will draft a letter based on this feedback and submit it, with a cancellation instrument, to the issuing Department for signature (usually by a senior official rather than the Secretary of State).

[2] Underlining in the original.

[Exhibit 3]

The underlined parts of this document indicate that it has been gisted for OPEN

Updated: January 2015

ISA Section 7 guidance

ISA authorisations

An ISA s7 authorisation given by the Secretary of State is the legal instrument that removes criminal liability in the UK for GCHQ actions overseas which might otherwise be an offence in UK law. Such an authorisation is also capable of removing any civil liability in the UK that might arise as a result of GCHQ's actions overseas. GCHQ primarily uses s7 authorisations for CNE operations. An ISA s7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations. Wherever possible, GCHQ seeks to rely on class authorisations with an underlying system of internal approvals.

The Section 7 Guidance sets out the 'class authorisations' signed by the Secretary of State under section 7 of the ISA which are used by GCHQ for the majority of its active internet-related operations. In respect of the authorisations relevant to CNE the Section 7 Guidance states that it permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant). The interference includes CNE operations.

Class authorisations are signed by the Foreign Secretary and need to be renewed every six months. Relevant personnel in GCHQ are responsible for overseeing the renewal process. Prior to expiry of the authorisations, they will ask analysts to briefly (re)justify the necessity and proportionality of continuing to rely on all extent section 7 internal approvals for which they are the lead, as well as asking for feedback on the outcomes of operations conducted. Providing feedback to the Foreign Secretary on the value of operations conducted under the class authorisations is crucial in justifying their renewal.

ISA section 7 internal approvals

A condition of section 7 class authorisations is that GCHQ operates an internal section 7 approval process to record its reliance on these authorisations. Before tasking the operational team to conduct CNE operations, analysts are required to complete a request form including a detailed business case described the necessity and proportionality of conducting operations against the targets. The request also sets out the likely political risk. The request must be endorsed by a senior member of the operational team before it is passed to an appropriately

senior official for approval. A copy of the signed final version of the approval is sent to FCO for information. This process provides the necessary reassurance to FCO that operations carried out under the class authorisations are necessary, justified and proportionate. Under a section 7 internal approval sits a third layer of authorisation: Additions (see below for details).

Section B – business case/necessity/proportionality:

The business case should include:

- the intelligence background;
- the priority in the priorities framework;
- an explanation of why the operations against the target set are necessary;
- the intelligence outcome(s) the proposed CNE activities are expected to produce.

You should also consider the level of intrusion the proposed operations will involve and how proportionality will be maintained. Key points to consider include:

- the expected degree of intrusion into a target's privacy and whether any personal or private information will be obtained;
- the likelihood of collateral intrusion, i.e. invading the privacy of those who are not targets, such as family members;
- whether the level of intrusion is proportionate to the expected intelligence benefit;
- any measures to be taken to ensure proportionality.

Based on all the information provided, relevant personnel will ensure that the section 7 internal approval is suitable for referral to an appropriately senior GCHQ official for signature. That official will review all the matters relevant to the application to satisfy himself that the proposed activity is justified, necessary and proportionate, including validating the assessment of political risk. He will also set the review period for the internal approval, which will be shorter for particularly sensitive operations.

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

Cancelling a section 7 internal approval

To show due diligence and as a condition of relying on the class authorisations, section 7 internal approvals should be cancelled when an operation is no longer needed. To help ensure that this happens, the relevant personnel will ask whether section 7 internal approvals are still needed as part of the class authorisation renewals process, and if so will seek a brief rejustification of the continuing necessity and proportionality. The number of approvals signed or cancelled is provided to the Foreign Secretary with the case for renewal.

It is important to cancel an internal approval as soon as it is no longer required.[1]

When a section 7 internal approval is no longer required, the analyst should ask the operational team point of contact to cease operations and remove all tasking. The relevant personnel will not formally cancel the approval until the operational team confirms that the operation is fully drawn down.

Reviewing section 7 internal approvals

In addition to the reviews that are carried out in support of the renewal of the class authorisations when analysts are required to briefly (re)justify the necessity and proportionality of continuing to rely on all extant internal approvals for which they are the lead, there is a rolling programme of fully revalidating all extant section 7 internal approvals. This revalidation mirrors the process for obtaining a new internal approval: an updated business case (covering justification, necessity, proportionality and intrusion into privacy) is provided by the lead analyst; the operational team confirm that they are still operating within the risk thresholds set when the internal approval was signed; the endorser confirms that the assessment of the likely political risk is still correct; then continued operations may be approved and a new review date set if no significant changes have been made (or the review of the approval is passed to a GCHQ official of appropriate seniority.)

New review history and cancellation forms will be appended at each review point. The intention is to leave the original submission intact, so that there is an audit trail of what was originally submitted/approved. If there are any updates to be made, these will be included in the review history so that there is an ongoing record at each review of what was decided and why.

A monthly summary report which summarises new s.7 approvals, reviews of s.7 approvals and cancellations, and also attaches copies of new approvals, is also sent to the relevant senior official at the FCO.

[1] Underlining in the original.

[Exhibit 4]

The underlined parts of this document indicate that it has been gisted for OPEN

Extract from current Advanced Training for Active Operations

CNE involves gaining remote access to computers and networks and possibly modifying their software without the knowledge or consent of the owners and users with the aim of obtaining intelligence.[1]

CNE operations must be authorised under ISA s.5 or s.7, depending whether the target computer or network is located within or outside the British Islands.

If you're working under a s.7 authorisation and find that the target computer has been brought to the UK, you should inform the relevant team immediately.

ISA permits a period of 5 working days before the presence of the implanted computer in the UK makes our action unlawful. You will have to fill out a form to register that you are in the "5-day grace period" and you may need to seek a s.5 warrant before the period expires.

No specific authorisation is required for developing CNE implants and techniques (no unauthorised access occurs), but testing may require authorisation. [2]

CNE operations carry political risk. These risks are assessed by the relevant team – consult them at an early stage if you're considering a CNE operation.

---

[1] Underlining in original.
[2] Both instances of underlining in this paragraph are in the original.

[Exhibit 5]

Summary of differences between current and previous versions of Section 5 and Section 7 Guidance

An earlier version of the Section 5 Guidance was created in July 2013 and first available to GCHQ staff from August 2013. There were no material differences between it and the current Section 5 Guidance.

Prior to that, there was an earlier version of the Section 5 Guidance, which was made available to GCHQ staff in June 2010. The only material difference between that version and the current Section 5 Guidance was that, while the requirement of proportionality was stipulated, the guidance did not give examples of considerations to be taken into account when assessing proportionality.

Prior to that advice on completing a s.5 template warrant was made available to staff in June 2009. This was practical advice on completing a warrant.

An earlier version of the Section 7 Guidance was available to GCHQ staff from August 2011. The material differences between that version and the current Section 7 Guidance were:

- While the requirement of proportionality was stipulated, the August 2011 guidance did not give examples of considerations to be taken into account when assessing proportionality;

- The August 2011 guidance did not address the review process for internal approvals, or cancellations of internal approvals; and

- The August 2011 guidance did not specify the need to rejustify the necessity and proportionality of relying on existing section 7 internal approvals as part of the class authorisation renewal process.

Prior to that, guidance in relation to Section 7 was contained within the form for requesting an internal approval. In the version available from September 2008, this explained the requirements that a CNE operation be justified (i.e. meets one of GCHQ's authorised functions), necessary (i.e. cannot be achieved more effectively through other means) and proportionate (i.e. restricts the interference to the minimum necessary to achieve the desired outcome and avoids collateral intrusion as far as possible).