IN THE HIGH COURT OF JUSTICE **Claim No.**
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT
London

B E T W E E N:

THE QUEEN on the application of

PRIVACY INTERNATIONAL

Claimant

-and-

INVESTIGATORY POWERS TRIBUNAL

Defendant

-and-

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

Interested Parties

STATEMENT OF FACTS AND GROUNDS

Suggested pre-reading:

Judgment of Investigatory Powers Tribunal, 12 February 2016

Report of the Intelligence Services Commissioner for 2014, Section 4iii (pp17-19)

A. Summary

1. This claim for judicial review raises two important issues of law:

   a) Is the Investigatory Powers Tribunal amenable to judicial review?

   b) Does section 5 of the Intelligence Services Act 1994 permit the issue of a 'thematic' computer hacking warrant authorising acts in respect of an entire class of property or people, or an entire class of such acts?

2. Computer hacking (known within the security and intelligence services as 'CNE', computer network exploitation) is a highly intrusive activity. When deployed against an

individual's computer or telephone, CNE can achieve results that are at least as intrusive as if the targeted individual were to have his house bugged, his home searched, his communications intercepted and a tracking device fitted to his person.

3. The degree of intrusion was summarised by Chief Justice Roberts in *Riley v California* in the Supreme Court of the United States. The basic point is that "*a cell phone search would typically expose to the government far more than the most exhaustive search of a house*…" As Roberts CJ explained:

> "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video — that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier…"

4. Further, CNE techniques can be deployed against entire networks of communications infrastructure, giving access to numerous computers at once. The consequence is the ability to gain bulk access to the data of very large numbers of people. CNE may also be used to alter commonly used computer software.

5. The Claimant brought proceedings in the IPT challenging various aspects of the use of CNE by GCHQ as contrary to domestic law and the European Convention on Human Rights. One of the aspects of the challenge was that:

a) Section 5 ISA 1994, the statutory power relied upon as justifying CNE within the British Islands[1], only empowered the Secretary of State to authorise "*the taking […] of such action as is specified in the warrant in respect of any property so specified*";

b) The Intelligence Services Commissioner (Sir Mark Waller) had disclosed in his 2014 Report [C/7/278] that the agencies had used section 5 "*in a way which seemed to me arguably too broad or 'thematic'*", and that the agencies had advanced and acted upon an interpretation of section 5 under which "*the property does not necessarily need to be specifically identified in advance*"; and,

c) Section 5 was not capable of supporting that broad interpretation.

6. In support of that argument, the Claimant relied on, amongst other things, the long-established hostility of the common law to 'general warrants', or any warrant which leaves questions of judgment to the person with authority to execute the warrant rather than the person with authority to issue it. The Claimant argued that that principle, recognised in celebrated cases such as *Entick v Carrington* (1765) 2 Wilson KB 275, *Money v Leach* (1765) 3 Burr 1742 and *Wilkes v Wood* (1763) Lofft 1, should not be taken to have been displaced by Parliament in the absence of clear words. The Claimant also relied on Article 8 of the European Convention on Human Rights.

7. The Government's position was that warrants of the type which had been held to be unlawful in *Entick*, *Money* and *Wilkes* are permissible under the power which Parliament had enacted in s. 5 ISA 1994.

8. On 1-3 December 2015, the IPT held an open hearing to determine issues of law and gave judgment on 12 February 2016 [C/5]. The IPT accepted the Government's submissions. It held at paragraph 37 [C/5/195]:

> "Eighteenth Century abhorrence of general warrants issued without express statutory sanction is not in our judgment a useful or permissible aid to construction of an express statutory power given to a Service, one of whose principal functions is to further the interests of UK national security, with particular reference to defence and foreign policy."

[1] Defined in schedule 1 to the Interpretation Act 1978 as meaning the United Kingdom, the Channel Islands, and the Isle of Man.

9. In essence, the IPT decided that the principle of legality, a long-established principle of construction in cases where it is alleged that legislation has interfered with important rights, does not apply to legislation concerning matters of national security. The IPT went as far as to hold that the common law abhorrence of a general warrant was not even a "*permissible aid to construction*" of a statutory power designed to "*further the interests of UK national security*".

10. It is submitted that that proposition is wrong in law. The principle that "*fundamental rights cannot be overridden by general or ambiguous words […] because there is too great a risk that the full implications of their unqualified meaning may have passed unnoticed in the democratic process*" (per Lord Hoffmann in R v SSHD ex parte Simms [2000] 2 AC 115 at 131) is at least as necessary in the context of national security as in any other context. The fact that the powers conferred in ISA 1994 are necessarily exercised in secret makes it all the more important that any grant of a power to interfere with fundamental rights is clear on the face of the statute so that its implications can be assessed. S.5 ISA 1994, in authorising the issue of warrants to take specified action in respect of specified property, should not be construed as permitting broad authorisations of whole classes of activity at once with no real specification at all.

11. That conclusion is also required by Article 8 of the Convention, together with s.3 Human Rights Act 1998. Article 8 requires that any interference with a person's private and family life, home, or correspondence must be "*in accordance with the law*". The case law makes clear that the power to engage in such interference must be subject to safeguards. If a 'thematic warrant' can ever comply with Article 8[2], strong and effective independent safeguards would be required. At the very least, the case law indicates that the decision as to necessity and proportionality be placed in the hands of an independent judicial authority, or a body which is independent of the executive.[3] In order to properly assess necessity and proportionality, the independent decision maker must be able to scrutinise the individualised suspicion that attaches to each target of the interference – the identified individuals, property or set of premises. Otherwise, that discretion would be

[2] As to which the Claimants expressly reserve their position, given the substantial pending litigation on related issues before the ECtHR and the CJEU.

passed to those implementing the warrant. S.5 ISA 1994 (as interpreted by the IPT) lacks any such safeguards; it permits the issue of warrants by the Secretary of State for a whole class of activity or range of property without judicial or independent approval. Accordingly, if the section had the wide scope which the IPT concluded it did, the United Kingdom would be in breach of Article 8. S.3 HRA 1998, which requires that legislation be read and given effect in a way which is compatible with the Convention rights. S. 5 therefore requires a narrow interpretation in order to avoid such a breach.

B. Facts

12. CNE is a powerful and intrusive surveillance technique. It therefore requires strong safeguards over its use. The key features of CNE are as follows:

a) **First**, the amount of information that can be derived through CNE techniques is large, and the nature of that information can be extremely sensitive. While interception of communications will result in the acquisition of information which an individual has chosen to communicate over a network, CNE may obtain information that a user has chosen not to communicate, for instance:

i) photos or videos stored on the device;

ii) documents;

iii) address book;

iv) location, age, gender, marital status, finances, ethnicity, sexual orientation, education and family; and

v) information collected through activation of the device's microphone or camera without the user's consent.

b) The agencies have the technological capability to acquire all such information from a user's device. David Anderson QC in his report *A Question of Trust* refers

[3] See *Szabo and Vissy v Hungary* (Application No 37138/14, 12 January 2016), §69, and *Kennedy v United Kingdom*

to documents disclosed by Edward Snowden which explain several of these capabilities used by GCHQ: "*a programme called NOSEY SMURF which involved implanting malware*[4] *to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured malware remained hidden*." [C/9/347]

c) **Secondly**, CNE involves an active intrusion into a device or network. CNE techniques are not limited to the acquisition of information; they can be used to amend, add, modify or delete information, or to instruct the device to act or respond differently to commands.

d) **Thirdly**, CNE allows for intrusion on a large scale. As well as specific devices, CNE can be used against networks of computers, or network infrastructure such as websites or internet service providers.

e) CNE can also be used against software, altering widely-used programs. For example, it appears that GCHQ has sought to modify or reverse-engineer commercially available software such as anti-virus software, having sought and apparently obtained a warrant under s.5 ISA 1994 authorising "*all continuing activities which involve interference with copyright or licensed software*" [C/10/350, 351/§7]

f) **Fourthly,** CNE may leave users vulnerable to further damage:

   i) Malware installed on a device can be used by third parties with similarly intrusive effects or worse.

   ii) The process necessary to install the malware without alerting the user or his security software may result in or preserve security vulnerabilities that could be exploited by third parties.

(2011) 52 EHRR 4, §160. Independent judicial authorisation is also required in other circumstances.
[4] A portmanteau word: malicious software.

iii) If the CNE takes place on a large scale – for instance in relation to network infrastructure, software, or common security protocols – it weakens security for all users, increasing the risk of exploitation by a third party.

C. Legal Framework

13. The detailed legal framework is set out at Annex 2 below. The key provisions are sections 5 and 7 ISA 1994.

14. Section 5 ISA provides:

> "(1) 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.
>
> (2) The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, 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 the Secretary of State—
>
> (a) thinks it necessary for the action to be taken for the purpose of assisting, as the case may be,—
>
> (i) the Security Service in carrying out any of its functions under the 1989 Act; or
>
> (ii) the Intelligence Service in carrying out any of its functions under section 1 above; or
>
> (iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and
>
> (b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;
>
> (c) is satisfied that satisfactory arrangements are in force under section 2(2)(a) of the 1989 Act (duties of the Director-General of the Security Service), section 2(2)(a) above or section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any

information obtained under the warrant will be subject to those arrangements. […]

(3) A warrant issued on the application of the Intelligence Service or GCHQ for the purposes of the exercise of their functions by virtue of section 1(2)(c) or 3(2)(c) above may not relate to property in the British Islands. […]"

15. Section 7 ISA provides:

> "(1) 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. […]
>
> (4) Without prejudice to the generality of the power of the Secretary of State to give an authorisation under this section, such an authorisation –
>
> (a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified,
>
> (b) may be limited to a particular person or persons of a description so specified, and
>
> (c) may be subject to conditions so specified. […]"

16. In summary:

a) Section 5 establishes a regime which can authorise interference with property within the British Islands, and which requires the issue of a warrant which must specify the action to be taken and the property in respect of which it will be taken; and,

b) Section 7 establishes a regime which cannot ordinarily authorise interference with property within the British Islands, but which simply requires an "*authorisation*" which may identify the authorised acts by "*description*".

c) Parliament therefore used clear words to grant permission for a class authorisation under section 7. No such words appear in section 5.

D. Thematic warrants

17. Because the activities of the agencies are necessarily conducted in secret, the manner in which section 5 ISA 1994 has been applied and the warrants which have been issued under it are largely secret. The Claimant, the public and the Courts are therefore reliant on the limited information which has been disclosed pursuant to (i) the review and reporting mechanisms which operate in relation to the agencies' activities, and (ii) the unauthorised disclosure of documents by the former NSA contractor Edward Snowden.

18. The issue of construction of section 5 ISA before the Court was accurately identified and properly brought to public attention by Sir Mark Waller, the Intelligence Services Commissioner, in his 2014 Report, published on 25 June 2015 [C/7/278]:

> "• Thematic Property Warrants
>
> I have expressed concerns about the use of what might be termed 'thematic' property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers 'to a particular act' or to 'acts' undertaken in the course of an operation. However, section 5 is narrower referring to 'property so specified'.
>
> During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or 'thematic'. I have expressed my view that:
>
> - section 5 does not expressly allow for a class of authorisation; and
> - the words 'property so specified' might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals.
>
> The agencies and the warrantry units argue that ISA refers to action and properties which 'are specified' which they interpret to mean 'described by specification'. Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which 'specifies' property by reference to a described set of persons, only being able to identify with precision an individual at a later moment".

19. Sir Mark Waller noted that the agencies' interpretation was "*very arguable*". He accepted "*in practical terms the national security requirement*", but went on:

"The critical thing however is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality. Thus I have made it clear:

- a Secretary of State can only sign the warrant if they are able properly to assess whether it is necessary and proportionate to authorise the activity
- the necessity and proportionality consideration must not be delegated
- property warrants under the present legislation should be as narrow as possible; and
- exceptional circumstances where time constraints would put national security at risk will be more likely to justify 'thematic' warrants.

This has led to one of the agencies withdrawing a thematic property warrant in order to better define the specified property."

20. It is clear from Sir Mark Waller's report that the agencies contend that s.5 ISA 1994 does not require that the property "*be specifically identified in advance*", and have acted upon their interpretation.

21. The Claimants do not know how many warrants have been issued in reliance upon that interpretation.

22. An indication of the type of warrants which may have been issued in reliance on that interpretation, however, is given by a GCHQ warrant renewal application dated 13 June 2008 which was disclosed by Edward Snowden [C/10/350]. The application says:

a) At paragraph 1: "*GCHQ seek a renewal of warrant GPW/1160 issued under section 5 of the Intelligence Services Act 1994 in respect of interference with computer software in breach of copyright and licensing agreements.*"

b) At paragraph 4: GCHQ's activity "*may involve modifying commercially available software [….] These actions, and others necessary to understand how the software works, may represent an infringement of copyright. The interference may also be contrary to, or inconsistent with, the provisions of any licensing agreement between GCHQ and the owners of the rights in the software.*"

c) At paragraph 7: "*The purpose of this warrant is to provide authorisation for all continuing activities which involve interference with copyright or licensed software, but which cannot be said to fall within any other specific authorisation held by GCHQ and which are done without the permission of the owner.*"

d) At paragraph 16 (the full text of the section under the heading 'Risk Assessment'): "*The risk of any interference such as that described in paragraph 4 becoming apparent to the owner of copyright or licensing rights is negligible.*"

23. It appears from that application that GCHQ sought and had previously been granted a general warrant permitting GCHQ to interfere with any computer software whatsoever, by any author, and in any circumstances.

E. Decision of the IPT

24. The IPT noted the concern that had been expressed by Sir Mark Waller, and at paragraph 35 set out the Claimants' submissions, including:

a) that the common law is hostile to general warrants "*as is well known from the seminal Eighteenth Century cases*", and that the principle of legality requires that "*fundamental rights cannot be overridden by general or ambiguous words*";

b) that s.5 was enacted in different terms from s.7, with the former requiring a warrant which specified the acts to be carried out and the property to be interfered with, and the latter containing no such requirement; and,

c) that s.5 requires that it "*be possible to identify the property/equipment at the date of the warrant*", so that the Secretary of State can consider whether the specific intrusion proposed is justified.

25. At paragraph 36 it set out the Government's submissions, including:

a) that the common law cases were "*at best of marginal relevance*" because they related to limitations on common law powers;

b) that the wording of s.7 was irrelevant to the construction of s.5 because it is a "*different provision […] and is not in direct contrast with, or alternative to, s.5*"; and,

c) that the requirement of s.5 was "*for the actions and property to be objectively ascertainable*", regardless of whether they are ascertainable by the Secretary of State at the time he or she decides to issue the warrant: "*A warrant could cover, in the examples given, anyone who was at any time during the duration of the warrant (six months unless specifically renewed) within the defined group*."

26. The IPT concluded at paragraph 37:

> "We accept Mr Eadie's submissions. Eighteenth Century abhorrence of general warrants issued without express statutory sanction is not in our judgment a useful or permissible aid to construction of an express statutory power given to a Service, one of whose principal functions is to further the interests of UK national security, with particular reference to defence and foreign policy. The words should be given their natural meaning in the context in which they are set."

27. At paragraph 38 it held that the test for whether a warrant complied with the requirement of specification was: *"Are the actions and the property sufficiently identified?"*

28. At paragraph 39 it contrasted the terms of s.5 ISA 1994 with the Evidence (Proceedings in Other Jurisdictions) Act 1975 (not cited by or the subject of submissions by either party), which provides that a letter of request must be for "*particular documents specified*": *"There is no requirement here for specification of particular property, but simply for specification of the property, which in our judgment is a word not of limitation but of description, and the issue becomes one simply of sufficiency of identification."*

29. At paragraphs 44 and 45 it held:

> "44. Given the width of meaning contained in the words 'action' and 'wireless telegraph' and, at least potentially, in the word 'property', specified cannot have meant anything more restrictive than 'adequately described'. The key purpose of specifying is to permit a person executing the warrant to know when it is being executed that the action which he is to take and the property or wireless telegraphy with which he is to interfere is within the scope of the warrant.
>
> 45. It therefore follows that a warrant issued under s.5 as originally enacted was not required:

(i) to identify one or more individual items of property by reference to their name, location or owner or

(ii) to identify property in existence at the date on which the warrant was issued.

Warrants could therefore, for example, lawfully be issued to permit GCHQ to interfere with computers used by members, wherever located, of a group whose activities could pose a threat to UK national security, or be used to further the policies or activities of a terrorist organisation or grouping, during the life of a warrant, even though the members or individuals so described and/or of the users of the computers were not and could not be identified when the warrant was issued."

30. Finally, at paragraph 47 it held:

> "In our judgment what is required is for the warrant to be 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 executing the warrant, so that the property to be covered is objectively ascertainable."

F. Summary of the IPT's conclusions

31. The IPT's analysis permits 'thematic' warrants of exceptional breadth. If the IPT were correct, it would be permissible in principle to issue a section 5 warrant to authorise property interference/CNE in the UK over:

a) "all mobile telephones in the United Kingdom";

b) "all computers used by anyone suspected by officials to be a member of a drug gang";

c) "all copies of Microsoft Windows used by a person in the UK who is suspected of having travelled to Turkey in the last year"; or

d) "all software obtained or used by GCHQ" (as, it appears from the very limited documents available to the Claimant, is the scope of the warrant which GCHQ sought in June 2008).

32. The effect of the IPT's decision is that a warrant can now be granted in identical terms to those granted in the general warrant cases (e.g. a "*strict and diligent search for the… authors printers and publishers of the aforesaid seditious libel intitled The North Briton… and them or any of them having found, to… seize… their papers*" (Money v Leach (1765) 3 Burrow 1742, 97 ER 1075)

33. On that interpretation, the decision as to whether a particular item of property falls within the description would be wholly for the person executing the warrant. The Secretary of State would retain no control over it, and because the terms of the warrant are secret there could be no real public scrutiny of how it has been applied. Further, evidence obtained through the actions authorised by the warrant would be admissible in Court, even though it had not been obtained with a judicial warrant.

G. Submissions

34. The IPT's expansive interpretation of section 5 ISA is wrong in law.

35. First, it collapses the careful distinction made by Parliament between a section 5 'warrant' and a section 7 'authorisation'.

a) Section 7 permits an authorisation of "*acts of a description*" or "*acts undertaken in the course of an operation so specified*" or acts affecting "*persons of a description so specified*". It therefore expressly permits the general authorisation of an entire operation, or a class of conduct. No similar wording permitting the authorisation of such wide classes or thematic operations is present in section 5.

b) The fact that Parliament adopted different formulations in relation to parallel powers in the same Act is relevant to how those formulations should be interpreted. If it had been intended that a warrant issued under section 5 could lawfully relate to property of a specified description, rather than specified property, there is no reason why the same formulation (and in particular the reference to "*description*") would not have been used in both section 5 and section 7.

c) The IPT's reliance on the terms of the Evidence (Proceedings in Other Jurisdictions) Act 1975 is misplaced. The fact that a different statute passed 29 years earlier used the words "*particular documents specified*" is far less relevant to the interpretation of s.5 than the fact that ISA 1994 itself adopted two different formulations in respect of two powers, one of which is exercisable by GCHQ within the United Kingdom and one of which is not.

36. Secondly, a 'thematic' warrant is a general warrant. It leaves the decision as to which property is to be interfered with (and what interference is to be carried out) to the person executing the warrant, rather than the person charged with the power to issue it. Hostility towards general warrants is a long-established principle of the common law, and so Parliament is only taken to have granted powers to issue a 'thematic' warrant if clear words are used, thus overriding the limits long respected by the common law on the proper scope of state interference with property within the jurisdiction:

a) Under the principle of legality, Parliament is taken not to have interfered with fundamental rights, unless it uses clear words. See *R v SSHD, ex parte Simms* [2000] 2 AC 115 at 131 per Lord Hoffmann:

> "Parliamentary sovereignty means that Parliament can, if it chooses, legislate contrary to fundamental principles of human rights. The Human Rights Act 1998 will not detract from this power. The constraints upon its exercise by Parliament are ultimately political, not legal. But the principle of legality means that Parliament must squarely confront what it is doing and accept the political cost. Fundamental rights cannot be overridden by general or ambiguous words. This is because there is too great a risk that the full implications of their unqualified meaning may have passed unnoticed in the democratic process. In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general words were intended to be subject to the basic rights of the individual. In this way the courts of the United Kingdom, though acknowledging the sovereignty of Parliament, apply principles of constitutionality little different from those which exist in countries where the power of the legislature is expressly limited by a constitutional document."

b) Although *Simms* concerned Article 10 of the European Convention on Human Rights, the effect of the principle is not limited to Convention rights, or even to

'rights' at all. As Lord Hobhouse said in R (Morgan Grenfell & Co Ltd) v Special Commissioners of Income Tax [2002] UKHL 21, [2003] 1 AC 563 at [44]:

> "The context in which Lord Hoffmann was speaking was human rights but the principle of statutory construction is not new and has long been applied in relation to the question whether a statute is to be read as having overridden some basic tenet of the common law."

c) A general warrant allows state officials, with no limits on time or place, to investigate a broad class of undesirable *conduct* (typically sedition in the 1700s, or a threat to national security now), rather than intrude on a specified *suspect* or *place*. In 1644, Coke condemned general warrants, as did Sir Matthew Hale in 1736. Hale explained that a "*general warrant to search in all suspected places is not good*" and "*not justifiable*" because it gave such discretion to mere Crown servants "*to be in effect the judge*" (History of the Pleas of the Crown, p. 150). Blackstone agreed, citing Money v Leach ("*a general warrant to apprehend all persons suspected, without naming or particularly describing any person in special, is illegal and void for it's uncertainty, for it is the duty of the magistrate and ought not to be left to the officer, to judge the ground of suspicion…*" (*Commentaries* Book IV, p. 288)).

d) Most of the leading common law property interference cases concern general warrants. The context was very similar to that of the present case. Often, it was argued that (to use modern language) there was an urgent threat to national security which required urgent action. In Entick v Carrington, it was argued of the seditious libel to which the warrant related that "*there can hardly be a greater offence against the State, except actual treason*". It may have been necessary and proportionate to issue a warrant covering an entire operation rather than specified property. But the common law did not accede:

   i) In Huckle v Money (1763) 2 Wilson 205, 95 ER 768 Lord Pratt CJ noted that: "*To enter a man's house by virtue of a nameless* [i.e. without specifying a named subject] *warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject*".

ii) In Wilkes v Wood (1763) Lofft 1, 98 ER 489 the Lord Chief Justice said: "*The defendants claimed a right, under precedents, to force persons houses, break open escrutores*[5]*, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject*."

e) In the absence of clear and express words, Parliament has not departed from the traditional limits on search and seizure within the UK, recognised as basic tenets of the common law in numerous celebrated cases and distinguished commentaries. The proper limits of a warrant are therefore those long recognised by the common law.[6]

f) Examples of the relevant limits are set out in the table at **Annex 1**. There is nothing objectionable in a warrant that defines its target by reference to a specified person or premises, rather than the specific items of property themselves. But legislation should not readily be construed as permitting a covert general warrant within the UK, in the absence of clear words.

g) Finally, if section 5 is ambiguous, reference to Hansard assists:

i) Sections 5(1) and 5(2) ISA are based on sections 3(1) and 3(2) of the Security Service Act 1989, which permitted the Secretary of State to issue a warrant "*authorising the taking of such action as is specified in the warrant in respect of any property so specified*". In promoting the Security Service Bill, John Patten MP, the Minister of State for Home Affairs, explained to

[5] In the modern world, escrutores have been replaced by computers and smartphones.

[6] The prohibition on general warrants was also incorporated into the Fourth Amendment to the US constitution ratified in 1792 ("*no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*"). This was the response to the wide use of writs of assistance, the standard form of general warrants in colonial America. Aware of the dangers of general warrants, the Virginia Declaration of 1776 also expressly forbade general warrants as "*grievous and*

Parliament that a warrant issued under this power could only authorise "*action in respect of a named property, and both the action and the name of the property must be on the warrant*" (HC Deb 17 January 1989 vol 145, col 269, underlining added).

ii) Equally, the Claimants have found nothing in the Parliamentary debates leading to the passing of the ISA to suggest that Parliament contemplated that a section 5 warrant could authorise interference with a class of property, specified by a broad description, as opposed to a specified item of property.

37. As set out above, the IPT's reasoning consisted of essentially two elements:

a) First, at paragraph 37, it rejected the relevance of the common law cases concerning warrants, holding: "*Eighteenth Century abhorrence of general warrants issued without express statutory sanction is not in our judgment a useful or permissible aid to construction of an express statutory power given to a Service, one of whose principal functions is to further the interests of UK national security, with particular reference to defence and foreign policy*."

b) Second, at paragraph 39, it held that "*there is no requirement here for specification of particular property, but simply for specification of the property, which in our judgment is a word not of limitation but of description, and the issue becomes simply one of sufficiency of identification*."

38. As to the first proposition:

a) The purpose of the principle of legality is to ensure that important rights are not abrogated by a statute whose "*full implications […] may have passed unnoticed in the democratic process*" (per Lord Hoffmann in Simms).

b) There is no good reason why that principle should cease to apply simply because the context of the statute is national security. In *Ahmed v HM Treasury* [2010] 2

---

oppressive". The Massachusetts constitution of 1780 followed – requiring "*special designation of the persons or objects of search, arrest or seizure*".

AC 534, a case concerning the freezing of assets belonging to individuals reasonably suspected of involvement in terrorism, the principle was applied with full force:

i) In the Court of Appeal the Treasury made submissions concerning the effect of general or ambiguous words in the United Nations Act 1946, and stressed "*the preventative nature of the regime introduced by the Security Council and the importance of avoiding terrorism*"; Sir Anthony Clarke held at [48]: "*For my part, I would not accept those submissions. I can see that the widest possible power might be desirable from the Government's point of view. I can also see that the public might take the same view. However, the principles which I have just stated are of fundamental importance*."

ii) The Supreme Court agreed. For example, Lord Hope expressly held at [75] that any interference with property required clear legislative words, citing the general warrant cases: "*the right to peaceful enjoyment of his property, which could only be interfered with by clear legislative words*: Entick v Carrington (1765) 19 State Tr 1029 , 1066, *per Lord Camden CJ… these rights are embraced by the principle of legality, which lies at the heart of the relationship between Parliament and the citizen. Fundamental rights may not be overridden by general words. This can only be done by express language or by necessary implication*". Arguments that national security cases should be treated differently were firmly rejected [79-80], noting the "*dangers that lie in the uncontrolled power of the executive*".

39. As to the second proposition:

a) S.5 ISA 1994 requires that the action and the property be "*specified*" in the warrant. Set against the background of the common law restrictions on powers of search and seizure, that clearly means that the person issuing the warrant must decide which specific property is to be the subject of the interference and confine the warrant to that property.

b) That is reinforced by the fact that s.7 contains no such requirements, instead contemplating that an 'authorisation' may be given in respect of "*acts of a description specified in the authorisation*" (emphasis added). S.5 does not provide that a warrant may be issued in respect of 'property of a description specified in the warrant'; it requires that the property be specified.

c) The IPT ignored the comparison between s.5 and s.7 ISA 1994 and instead relied on an unhelpful analogy with s.5 ISA 1994 and the Evidence (Proceedings in Other Jurisdictions) Act 1975, concluding that the absence of the word "*particular*" in s.5 ISA 1994 means that the requirement to specify property is simply a requirement to give a description.

d) That provision is not a useful aid to the construction of s.5, and in any event it does not outweigh the conclusion which is compelled by (i) the principle of legality, (ii) the importance to the common law that search and seizure powers be tightly circumscribed, (iii) the clarity of the words of s.5, and (iv) the fact that s.5 does not contain the much more general formulation adopted in s.7.

Article 8 ECHR

40. The interpretation of s.5 ISA 1994 for which the Claimant contends is also required by Article 8 ECHR, under which Member States must maintain certain minimum safeguards in relation to intrusive powers of surveillance.

41. The principle of legality applies to Convention rights as well as fundamental common law rights; as noted above, *Simms* concerned Article 10 ECHR. Further, s.3 HRA 1998 requires: "*So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.*"

42. Article 8 ECHR imposes significant safeguards which Member States must implement in relation to powers of surveillance. For example, in *Weber & Saravia v Germany* (2008) 46 EHRR SE5, the ECtHR recognised six "*minimum safeguards*" which "*should be set out in statute law*" in order for a secret surveillance power to be compliant (§95). Moreover, in *Szabo & Vissy v Hungary* (Application 37128/14, 12 January 2016), the ECtHR indicated that "*The guarantees required by the extant Convention case-law on interception need to be*

enhanced" in view of the impact of "*cutting-edge technologies*" on the scale and effect of such interception.

43. In particular, Article 8 ECHR does not permit the issue of a warrant authorising modern forms of intrusive electronic surveillance without prior authorisation by a court or other authority which is structurally and functionally independent of the authority seeking access. Moreover, that independent authority must be presented with evidence of individualised suspicion in order to be able to assess the necessity and proportionality of the interference proposed.

a) In *Weber* (above), the relevant power could only be exercised with prior authorisation, or in urgent cases *ex post facto* approval, from an independent commission: see §115.

b) In *Telegraaf Media* (Application No 39315/06, 22 November 2012), an interception of journalists' communications was held to violate Articles 8 and 10 ECHR because, although it was authorised by a Minister, it was done "*without prior review by an independent body with the power to prevent or terminate it*" (§100).

c) In *Szabo* (above), the ECtHR made clear at [77] that "*supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees*". Further, an independent authorising authority must be presented "*with a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of the necessity of the proposed measure – and this on the basis of an individualised suspicion regarding the target person*" [71]. Without such evidence of individualised suspicion, to be assessed by an independent authority, the ECtHR concluded at [71] that an "*appropriate proportionality test*" could not be carried out. It noted at [69] that the earlier case of *Kennedy v United Kingdom* (2011) 52 EHRR 4, in which the ECtHR had held that a regime of interception warrants was compatible with Article 8, had concerned a tightly circumscribed power – noted by the ECtHR in *Kennedy* at [160] as requiring the identification of one specific person or set of premises as the subject of the warrant – and was therefore not applicable where the power could potentially "*be taken to enable so-called strategic, large-scale interception*".

d) The case law of the CJEU in relation to Articles 7 and 8 of the EU Charter (which are analogous to Article 8 ECHR) similarly makes clear that any interference with personal data must be accompanied by certain minimum safeguards: see *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2015] QB 127 at [54-55] and *Schrems v Data Protection Commissioner* [2016] 2 WLR 873 at [91]. In particular, in *Digital Rights Ireland*, the CJEU held that Directive 2006/24 was invalid on grounds including (at [62]): "*Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.*"

44. If the power in s.5 ISA 1994 were as broad as the IPT has held, it would allow broad CNE operations to be authorised by the Secretary of State, in secret, with no judicial or independent authorisation either before or after the fact. That would be incompatible with Article 8 ECHR.

45. Further, if (as the IPT concluded) s.5 ISA 1994 permitted the Secretary of State to issue warrants leaving any discretion or matter of subjective judgment to the person executing the warrant, an intrusive act by that individual would not in substance have been authorised even by the Secretary of State, let alone by a judicial or independent body. That outcome is incompatible with Article 8 ECHR.

46. Nor is there any adequate *ex post* judicial supervision: the Intelligence Services Commissioner has no power to refer any warrant or excessive use of section 5 to the IPT, nor any power to disclose errors or misuse to the victim.

47. Accordingly, s.5 ISA 1994 must be construed as not permitting the issue of warrants of the type set out in the second part of Annex 1.

48. Alternatively, if the Court concludes that the statute cannot be read consistently with the requirements of Article 8, the Claimant seeks a declaration of incompatibility.

49. The requirement for prior judicial or independent authorisation was not argued in the IPT, because the IPT had held in a previous case (*Liberty and Privacy International v GCHQ* [2015] HRLR 2) that Article 8 did not require such authorisation. However, (i) the Claimant expressly reserved its position in the present proceedings as to the correctness of that decision (skeleton argument, footnote 8), and indeed is challenging it before the ECtHR, and (ii) in any event, the decision in *Szabo* (delivered in January 2016) makes clear that such authorisation is required.

H. 'Ouster clause'

50. Section 67(8) of RIPA 2000 provides, in relation to the IPT:

> "Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court."

51. The Claimant anticipates that the Defendant or the Interested Parties may contend that the effect of s.67(8) is to oust the Court's jurisdiction to hear this claim, on the basis that the IPT is not amenable to judicial review.

This is the first case in which the Administrative Court has been invited to hear argument as to the effect of section 67(8). In *A v B* [2009] EWCA Civ 24 the Court of Appeal considered whether the Tribunal had exclusive jurisdiction over a claim by a former member of the Security Service who wished to publish his memoirs.

a) Laws LJ commented at [22] that there was nothing constitutionally improper about a supervisory jurisdiction over the Security Services being exercised by a specialist tribunal, rather than the Courts. This is entirely correct, so far as it goes. But Laws LJ did not consider whether an error of law *by the Tribunal* could be corrected by way of judicial review. Laws LJ did not cite or consider the effect of section 67(8).

b) In the Supreme Court, Lord Brown (for the Court) adopted Laws LJ's analysis. He also commented, *obiter*, that section 67(8) was an "*unambiguous ouster*", but this appears to have been based on a concession by *A*. Lord Brown also noted

that the Court had heard no argument on the point: "*…but that is not the provision in question here…*"

52. Section 67(8) does not oust the supervisory jurisdiction of the High Court to hear a claim for judicial review of a purported decision of the IPT which is in error of law. It is well established that a decision in error of law is an act in excess of jurisdiction, and is therefore void. Such a purported 'decision' can therefore be challenged by way of judicial review. An 'ouster clause' does not prevent this. See *Anisminic v Foreign Compensation Commission* [1969] 2 AC 147 and de Smith's *Judicial Review*, 7th Ed. at para. 4-031.

53. In *Anisminic*, the 'ouster clause' was almost identical to section 67(8) of RIPA 2000. The only difference between the *Anisminic* 'ouster clause' and the RIPA version is the addition of the words "*(including decisions as to whether they have jurisdiction)*".

54. These additional words make no difference here. If the additional words in parentheses mean anything at all, they only seek to oust the supervisory jurisdiction of the Administrative Court in a case where the Tribunal has to decide whether it has jurisdiction to hear a particular case. There is no dispute that the Tribunal had jurisdiction to decide the issues set out above. The Tribunal was not making a decision in this case as to "*whether they have jurisdiction*", but instead making an erroneous and thus void 'decision' on a question of law. Like the 'ouster clause' in *Anisminic*, section 67(8) of RIPA only prohibits judicial review of an actual decision. It does not deal with a case where, because the Tribunal acted unlawfully, on a proper analysis there is no valid decision at all.

55. In any event, as a matter of constitutional principle, an attempt to oust the jurisdiction of the High Court in favour of an inferior tribunal will fail. The High Court is the only English and Welsh court with unlimited original jurisdiction. As a basic constitutional principle, its jurisdiction cannot be abrogated: *R (Cart) v Upper Tribunal* [2009] EWHC 3052 (Admin).

56. The reasons why common law courts approach ouster clauses with such concern are well understood. The risk is that "*a tribunal preoccupied with special problems or staffed by*

individuals of lesser ability is likely to develop distorted positions. In its concern for its administrative task it may strain just those limits with which the legislature was most concerned". The basic principle is therefore that a "*tribunal of limited jurisdiction should not be the final judge of its exercise of power; it should be subject to the control of the courts of more general jurisdiction*". See Jaffe *Judicial Review: Constitutional and Jurisdictional Fact* (1957) 70 *Harvard Law Review* 953 cited with approval by the High Court of Australia in *Kirk v IRC* [2010] HCA 1 at [64], dismissing an attempt to rely on an ouster clause far wider than section 67(8).

57. The present case is a good example of those concerns. The Tribunal has jurisdiction over claims against the intelligence and security services. It has rejected a principle of fundamental constitutional importance and general application concerning the interpretation of Acts of Parliament on the grounds that that principle is unsuited to the context of national security in which the intelligence and security services operate. That is a distorted position as to the exceptionality of the sphere in which the Tribunal operates, and it has produced a clear error of law which the courts ought to correct.

I. Protective Costs Order

58. Finally, the Claimant seeks a Protective Costs Order on the grounds that the litigation raises issues of general public importance, and the Claimant will be unable to proceed with the claim unless it is so protected. See the witness statement of Barry Kernon, the Claimant's Treasurer, at [B/1].

59. Proceedings before the IPT are conducted without the risk of costs following the event of an adverse determination. As the Tribunal records on its website at http://www.ipt-uk.com/section.aspx?pageid=26: "*The Tribunal has never awarded costs and its present view is that its jurisdiction to do so, if it exists at all, would be exercised only in exceptional cases. […] Complainants should therefore assume that the likelihood is that no costs will be awarded.*" Further, the Claimant's legal team acted *pro bono* in the IPT. The Claimant was therefore able to raise the issue before the IPT without any costs risk.

60. However, the Claimant now seeks an authoritative determination from the High Court as to whether one important aspect of the IPT's decision is wrong in law.

61. In *R (Corner House Research) v Secretary of State for Trade and Industry* [2005] EWCA Civ 192, [2005] 1 WLR 2600, the Court of Appeal held:

> "A protective costs order may be made at any stage of the proceedings, on such conditions as the court thinks fit, provided that the court is satisfied that: (i) the issues raised are of general public importance; (ii) the public interest requires that those issues should be resolved; (iii) the applicant has no private interest in the outcome of the case; (iv) having regard to the financial resources of the applicant and the respondent(s) and to the amount of costs that are likely to be involved, it is fair and just to make the order; and (v) if the order is not made the applicant will probably discontinue the proceedings and will be acting reasonably in so doing."

62. The first and second criteria are clearly satisfied. The claim raises issues of general public importance as to the extent of the powers of the security and intelligence services to carry out computer hacking. That issue has been of real public concern since the Snowden disclosures revealed something of the extent and scope of that activity. It is likely that the public and most of Parliament were unaware that s.5 ISA 1994, an Act concerning interferences with specified property enacted when computers were much less common and held far less data than today, was being used as the sole legal basis for wide-ranging 'thematic' CNE operations in the United Kingdom, including apparently for a general authorisation permitting interference with intellectual property and contractual rights in software. It is in the public interest that the Court determine whether that Act abrogated the general common law constraints on powers of interference with property in the manner alleged.

63. The third criterion is also plainly satisfied; the Claimant is a charity and has no private interest in the outcome of the litigation.

64. As to the fourth and fifth criteria:

a) As set out in Mr Kernon's witness statement, the majority of the Claimant's funds are restricted for use for particular purposes. Its unrestricted income in the year ending 31 January 2016 was £65,954 [B/1/6/§14]. In addition to bearing the costs of court fees and copying, it is able to risk £10,000 of its unrestricted funds

as a contribution towards any costs order made in the proceedings, and anticipates a further £5,000 being raised externally for that purpose through fundraising activities. It therefore seeks an order prospectively capping its adverse costs liability at £15,000.

b) As Mr Kernon says at paragraph [B/1/10/§35], the Claimant's trustees have concluded that it will not be able to proceed with the litigation unless its costs are so capped. In view of the financial information he presents, that is a reasonable conclusion. The result would be that an important issue of legal principle will not be determined.

c) Finally, the Claimant's counsel and solicitors are acting in these proceedings on conditional fee agreements, with their fees capped at Treasury rates and with no entitlement to be paid any fees unless the claim succeeds.

J. Conclusion

65. The Court is invited to grant permission and a protective costs order, and in due course quash the IPT's declaration as to the proper scope of section 5 ISA, substituting a correct declaration as to the law under section 31(5) of the Senior Courts Act 1981.

DINAH ROSE QC

BEN JAFFEY

TOM CLEAVER

Blackstone Chambers

BHATT MURPHY

9 May 2016

Annex 1: Proper limits to the use of section 5 ISA

Scenario	Within s5 ISA?	Comments
Mobile phone with serial number ABC123	Yes	
Mobile phone used by Smith	Yes	
All mobile phones used by Smith	Yes	May cover more than one item of property, expressly described in the warrant
All mobile phones used by Smith or Bloggs	Yes	May cover more than one person's property, expressly described in the warrant
All mobile phones used by the blonde-haired man approximately 5ft 10 tall (name unknown) seen leaving 1 Acacia Avenue at midday on 1 December 2015	Yes	May not know the true identity of person, but property is objectively ascertainable. An interference with the wrong person's property would be unlawful
All mobile phones used by persons who at today's date are on the FCO Syrian diplomatic list	Yes	Persons are objectively ascertained at point of warrant grant. No more than shorthand for a list of names in a schedule
All computers at 1 Acacia Avenue	Yes	May be described by reference to a set of premises
All computers at 1 and 2 Acacia Avenue	Yes	May cover more than one person's property, expressly described in the warrant

All mobile phones used by suspected members of Al-Qaeda	No	Leaves decision and discretion as to intrusion to official, not the Secretary of State authorising a warrant.
All mobile phones used by suspected associates of members of Al-Qaeda	No	Leaves decision as to intrusion to official.
"*All continuing activities which involve interference with copyright or licensed software, but which cannot be said to fall within any other specific authorisation held by GCHQ and which are done without the permission of the owner*"	No	Indeterminate class. Leaves decision as to what property will be intruded in to official, and cannot be determined at time of warrant issue. This is an authorisation of an *operation*, permissible under section 7 ISA, but not section 5.
All mobile telephones in Birmingham	No	Indeterminate class. Cannot determine from warrant the property to which it will be directed.
A "*strict and diligent search for the… authors printers and publishers of the aforesaid seditious libel intitled* The North Briton*… and them or any of them having found, to… seize… their papers*" (*Money v Leach* (1765) 3 Burrow 1742, 97 ER 1075)	No	Leaves decision as to intrusion to official. A general warrant authorising an *operation* not a search of specified property.

Annex 2 – Legislative Framework

Intelligence Services Act 1994

66. Section 3(1)(a) ISA provides that GCHQ's functions include "*to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material*". Section 3(2) ISA stipulates that these functions are exercisable only in the interests of national security, the economic well-being of the United Kingdom, or the prevention or detection of serious crime.

67. Section 4(2)(a) ISA provides that one of the duties of the Director of GCHQ is to secure that "*no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings*".

68. Section 5 ISA provides:

> "(1) 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.
>
> (2) The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, 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 the Secretary of State—
>
> (a) thinks it necessary for the action to be taken for the purpose of assisting, as the case may be,—
>
> …
>
> (iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and
>
> (b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;

(c) is satisfied that satisfactory arrangements are in force under …section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements."

69. Section 5(3) ISA provides that a warrant authorising interference with property within the British Islands can only be issued to GCHQ for its functions in respect of national security or the economic well-being of the UK. Within the UK, the Security Service handles the prevention and detection of serious crime, although GCHQ may in practice act on its behalf in actually carrying out interference.

70. In relation to section 5 warrants, section 6 ISA provides:

a) at section 6(1), that warrants may only be issued under the hand of the Secretary of State or, in urgent cases, certain other officials;

b) at section 6(2), that warrants issued by the Secretary of State expire after six months unless renewed;

c) at section 6(3), that the Secretary of State may renew a warrant for 6 months at any time;

d) at section 6(3), that the Secretary of State shall cancel a warrant *"if he is satisfied that the action authorised by it is no longer necessary"* (Section 6(4)).

71. In contrast, section 7 ISA provides:

"(1) 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.

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom.

(3) The Secretary of State shall not give an authorisation under this section unless he is satisfied—

(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be

done will be necessary for the proper discharge of a function of the Intelligence Service or GCHQ; and

(b) that there are satisfactory arrangements in force to secure—

(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of the Intelligence Service or GCHQ ; and

(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and

(c) that there are satisfactory arrangements in force under section 2(2)(a) or 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

(4) Without prejudice to the generality of the power of the Secretary of State to give an authorisation under this section, such an authorisation—

(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified.

…

(9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which—

(a) is done in the British Islands; but

(b) is or is intended to be done in relation to apparatus that is believed to be outside the British Islands, or in relation to anything appearing to

originate from such apparatus."

Section 7 also sets out provisions for the issue, renewal and cancellation of warrants, which broadly mirror those for warrants issued under section 5.

72. The power under section 7 to authorise acts outside the British Islands is much broader than the power in section 5. In particular:

a) Section 7 is not limited to actions in respect of property or wireless telegraphy. It could be (and is) used to authorise a variety of other activities, including the recruitment of agents and the payment of bribes or inducements.

b) Section 7(4) permits the authorisation of acts by reference to a description of people or a class of operations, rather than merely in relation to "*specified*" property.

Police Act 1997

73. The ISA powers are very similar to the property interference powers available to the police under Part III of the Police Act 1997. The power to authorise interference is exercisable by senior police officers in their area, or more widely in certain cases:

a) section 93(1)(a) provides: "*Where subsection (2) applies, an authorising officer may authorise … the taking of such action, in respect of such property in the relevant area, as he may specify …*";

b) section 93(2) establishes two cumulative criteria: first, that the authorising officer believes "*that it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime*", and second, that the authorising officer believes "*that the taking of the action is proportionate to what the action seeks to achieve*"; and

c) the Act also provides for authorisations to be reviewed by independent judicial Commissioners appointed under section 91, and makes specific provision in relation to the protection of legally privileged information: sections 97 and 98.