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

THE RESPONDENTS' SKELETON ARGUMENT FOR OPEN PRELIMINARY ISSUES HEARING 1-4 DECEMBER 2015

Privacy International and the Greennet Claimants are referred to below as "the Claimants".
The term "Respondents" is used below to refer to both Respondents in both Claims.
The IPT judgment in the Liberty/Privacy proceedings, [2014] UKIPTrib 13_77-H dated 5 December 2014, is referred to in this Response as "the Liberty/Privacy judgment".

Where appropriate references to the hearing bundles and authorities' bundles have been included in square brackets and with the authorities shown as [A1/A2].

INTRODUCTION

1. This skeleton addresses the Open preliminary issues of law (1-5) which have been agreed between the parties. For ease of reference when considering these submissions, the Respondents have set out in an Appendix to this skeleton argument the matters which go to make up the relevant legal regime including the relevant statutory provisions, Codes and oversight mechanisms. The abbreviations used in that Appendix have been adopted in this skeleton argument.

2. Over the last year the threat to the UK from international terrorism has continued to increase. The threat level currently stands at SEVERE which means an attack in the UK is highly likely. Six alleged terror plots targeting the UK have been stopped in the year prior to September 2015.[1]

3. As is more than apparent from recent and tragic events in Paris, the principal terrorist threat derives from militant Islamist extremists, particularly in Syria and Iraq. Even before the attacks in Paris, it was clear that ISIL had emerged as the most violent of the terrorist groups operating in that region and that it was supported by foreign fighters from European countries[2]. And central to ISIL's operational successes is "*an unprecedented quantity of extremist and terrorist propaganda*"[3].

4. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging; and it is in that regard that GCHQ plays a leading role given its expertise in digital communications technology. A combination of factors including the increasing use of the internet and social media by groups like ISIL, the unprecedented security of terrorist communications and the advent of ubiquitous encryption, mean that the work required to tackle national security threats is getting harder.

5. Thus GCHQ and the other intelligence agencies must develop innovative and agile technical capabilities to meet these serious national security challenges. Computer Network Exploitation (CNE) is one such capability[4]. Its importance

[1] See §7 of the first witness statement of Ciaran Martin, Director of Cyber Security at GCHQ dated 16 November 2015 – Open Bundle, Section B, p124.
[2] Ibid §§7-8
[3] Ibid §8 and 10
[4] Ibid §20

relative to GCHQ's overall capabilities has been increasing in recent years and is likely to increase further[5]. Indeed, CNE may, in some cases, be the *only* way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country[6]; and without it GCHQ's ability to protect the UK from terrorism, cyber attack, serious crime (including child sexual exploitation) and a range of other threats would be seriously degraded.[7]

6. Contrary to the Claimants' assertions, CNE is lawful as a matter of domestic law and under the ECHR. There is a clear legal framework governing CNE activities, including the availability of warrants/authorisations under s.5 and s.7 ISA, supplemented in important respects by the CMA 1990, the HRA, the DPA, the OSA, the relevant Codes, GCHQ's internal arrangements and important oversight mechanisms. That regime is both accessible and has a proper basis in domestic law. It is a regime which provides for stringent safeguards if GCHQ wishes to carry out CNE activities. It is also proportionate given the need for CNE to be carried out to protect the public from serious terrorist and other threats.

7. The Claimants make extreme assertions about the intelligence gathering activities of GCHQ, including their alleged indiscriminate and arbitrary nature. Such assertions are flatly contradicted by eg. the recent report of the ISC[8] and the conclusions of the Intelligence Services Commissioner (Sir Mark Waller) who described GCHQ staff as acting "*with the highest level of integrity and legal compliance*" in his 2013 report[9] and noted in his 2014 report (with specific reference to the s.7 ISA process) that "*a great deal of thought was going into assessing the necessity of the activity in the national interest and to ensure privacy was invaded to the least degree possible*"[10].

8. Thus, whilst the NCND principle precludes GCHQ from responding to the factual allegations which are made in these proceedings (and which have been addressed thoroughly in CLOSED), it is denied that GCHQ is engaged in any unlawful and indiscriminate mass surveillance activities.

9. As to the specific preliminary legal issues to be addressed in this OPEN hearing, the Respondents' position on each is in summary as follows:

---

[5] Ibid §20
[6] Ibid §31
[7] Ibid §34
[8] In their report "*Privacy and Security: A modern and transparent legal framework*" dated 12 March 2015 the ISC stated, *inter alia*, that "*We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do"* (see (v) **Vol 1/CM1/p562**).
[9] Ibid §72
[10] Ibid §72

Issue 1 GCHQ's CNE activities have been lawful as a matter of domestic law both before and after 3 May 2015. Prior to 3 May 2015 an act constituting an offence under s.3 CMA 1990 was capable of being authorised by a warrant or authorisation under the ISA (or a RIPA warrant). In addition, even if the effect of the Criminal Justice Act 1948 is of more than academic interest in these proceedings, that Act does not extend the territorial reach of the CMA 1990 for Crown servants.

Issue 2 Section 5 ISA does permit the issue of a warrant where "property" is "specified" by description and such description may encompass more than one particular location, or item of property.

Issue 3 The power under s.5 ISA to authorise interference with "property" does extend to intangible legal rights such as copyright.

Issues 4/5 The regime which governs CNE is "*in accordance with the law/prescribed by law*" under Article 8(2)/Article 10(2) ECHR. It is sufficiently foreseeable, contains sufficient safeguards to protect against arbitrary conduct, is proportionate and this has been the case since 1 August 2009.

ISSUES 1-3 – DOMESTIC LAW

Issue 1: Prior to the amendments to the Computer Misuse Act 1990 ("CMA 1990") with effect from 3 May 2015, and after those amendments:
a. was an act constituting an offence under s.3 CMA 1990 capable of being rendered lawful by a warrant issued under the Regulation of Investigatory Powers Act 2000 ("RIPA 2000") or a warrant or authorisation under the Intelligence Services Act 1994 ("ISA 1994")?
b. would the CNE activities of a Crown servant in the course of his employment, if committed in a foreign country or against assets or individuals located in a foreign country, have amounted to an offence under s.3 CMA 1990 as though the activities had been committed in England and against assets or individuals located in England?

Is an offence under s.3 CMA 1990 capable of being rendered lawful by ISA/RIPA?

10. The Claimants contend that, prior to the amendments to the CMA 1990 on 3 May 2015, an act constituting an offence under s.3 CMA 1990 was not capable of being rendered lawful by any other enactment conferring powers of inspection/examination, search or seizure. In particular they assert that only lesser interferences, amounting to a breach of s.1 of the CMA 1990, could be

authorised by warrant under RIPA or the ISA (see §§37 and 41B(a) of Privacy's Re-Amended Grounds dated 13 July 2015[11]). It appears to be accepted from Privacy's Grounds (adopted by the Greennet Claimants[12]) that since amendments to the CMA 1990 were made in May 2015, conduct under s.3 of the CMA 1990 could be authorised by a warrant under RIPA/the ISA (see §41B of Privacy's Grounds). Consequently any live issue is confined to the position pre-May 2015.

11. When enacting the ISA in 1994, after the coming into force of the CMA in 1990, Parliament made specific provision for the Intelligence Services, including GCHQ, to conduct activities which might otherwise be unlawful (whether under criminal or civil law), where the activity was authorised by s. 5 warrants or s. 7 authorisations. That is made expressly clear by the language of the ISA, in particular at s.5(1) and s.7(1)-(2):

> *"5(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***.
>
> "7*(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.***
>
> *7(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****."*(emphasis added)

12. As regards GCHQ's activities, Parliament was also clear when enacting the ISA that such activities should include the monitoring or *interference* with any equipment producing electromagnetic, acoustic and other emissions, as expressly stated to be part of GCHQ's statutory functions in s. 3(1)(a) of the ISA. That language plainly includes interferences which would otherwise constitute an offence, including impairing the operation of a computer under s.3 of the CMA 1990.

13. Consequently, the specific statutory scheme in the ISA is structured such that both s.5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that they are not civilly or criminally liable for such interferences, including under the CMA 1990.

14. S.10 of the CMA (prior to being amended on 3 May 2015) did not have the effect that only lesser interferences, amounting to a breach of s.1 of the CMA,

[11] See Open Bundle Part A, at p17 and p21.
[12] See Open Bundle Part A, p58 at §63.

could be authorised, including under the ISA or RIPA. That section was directed at "*certain law enforcement powers*" (see the title to s. 10) i.e. powers of inspection, search or seizure (eg. by the police)[13]. It did not purport to set out exhaustively the circumstances in which, what would otherwise be offences under the CMA, might be authorised eg. by the Intelligence Services when exercising their statutory functions including in the interests of national security and the prevention and detection of serious crime.

15. It follows that the amendments to s.10 CMA were clarificatory only. That is confirmed by the explanatory notes to that section and by the Home Office Fact Sheet to the Serious Crime Act 2015 (Part 2: Computer Misuse) and the Home Office Circular, both dated March 2015, which stated as follows:

> "*Section 10 of the 1990 Act contains a saving provision. It provides that the offence at section 1(1) of the 1990 Act has effect without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure; and in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.* ***The amendment to section 10 of the 1990 Act made by this section is a clarifying amendment. It is designed to remove any ambiguity over the interaction between the lawful exercise of powers (wherever exercised) conferred under or by virtue of any enactment (and in Scotland, rule of law) and the offence provisions.*** *"Enactment" is expressly defined to provide certainty as to what this term includes. The title of section 10 of the 1990 Act has also been changed to remove the reference to "certain law enforcement powers" (see paragraph 12 of Schedule 4). This is to avoid any ambiguity between the title and the substance of that section.*" (Explanatory Notes, emphasis added[14])
>
> "*Section 44 clarifies the savings provision at section 10 of the 1990 Act and is intended to remove any ambiguity for the lawful use of powers to investigate crime (for example under Part 3 of the Police Act 1997) and the interaction of those powers with the offences in the 1990 Act. The changes do not extend law enforcement agencies' powers but merely clarify the use of existing powers (derived from other enactments, wherever exercised) in the context of the offences in the 1990 Act*." (Home Office Fact Sheet)
>
> "*Section 44 clarifies section 10 of the CMA. Section 10 of the CMA contained a saving provision whereby criminal investigations by law enforcement agencies did not fall foul of the offences in the Act. However, section 10 pre-dates a number of the powers, warrantry and oversight arrangements on which law enforcement now rely to conduct investigations, such as those in Part 3 of the Police Act 1997. The changes do not extend law enforcement agencies' powers but merely clarify the use of the existing powers (derived from other enactments, wherever exercised) in the context of the offences in the CMA*." (Home Office Circular)

16. The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect

[13] See **[A1/Tab 2]**
[14] See **[A1/Tab 12]**

unless there was an express savings provision in each relevant piece of legislation (whether governing criminal or civil liability), making clear that it was without prejudice to powers set out in any other enactment. That is manifestly inconsistent with the scheme of the ISA. It also elevates the status of savings provisions eg. in the CMA 1990, beyond that which is tenable. As has been recognised in the case law, savings provisions are a frequently unreliable guide to the provisions to which they attach, since savings provisions "*are often included by way of reassurance, for the avoidance of doubt or for an abundance of caution*" - see Lord Simon of Glaisdale in *Ealing London Borough Council v Race Relations Board* [1972] AC 342 at 363.

17. As to RIPA, it is to be noted that this would only be relevant if GCHQ's CNE activity also required a Part II RIPA warrant as well as an ISA warrant/authorisation eg. if intrusive surveillance was being carried out. But, in any event, RIPA came into force after the CMA 1990[15] and Part II, makes clear that conduct to which that chapter applies is "*lawful for all purposes*" if it is authorised under that Chapter (see s. 21(2)[16]).

18. Accordingly, the submissions at §37 and §41B(a) of Privacy's Amended Grounds are wrong in law.

Does s. 48 of the Criminal Justice Act 1948 ('the CJA') extend the scope of territorial jurisdiction of the CMA 1990 for Crown servants?

19. The Claimants contend that s. 31 of the CJA[17] has the effect of extending the territorial reach of the CMA 1990 for Crown servants. It is said that the effect of s.31 means that any breach of the CMA 1990 by a Crown servant abroad is deemed to have taken place in England and is within the territorial jurisdiction of the CMA 1990 (see §§37D, 37F, 41B(b) and 47A of Privacy's Amended Grounds).

20. The Respondents' primary submission is that the interface between the CJA and the CMA 1990 is entirely academic in circumstances where GCHQ has confirmed that, as a matter of practice, any CNE activities carried out abroad, or over a foreign computer, even if the relevant user is located in the United Kingdom, would be authorised by a s. 7 ISA authorisation (see §146C(a) of

[15] Section 3 of the CMA 1990 came into force on 29 August 2000 and RIPA 2000 came into force on 2 October 2000.
[16] See **[A1/Tab 10]**
[17] Which provides as follows: "*31(1) Any British subject employed under His Majesty's Government in the United Kingdom in the serviced of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence and subject to the same punishment, as if the offence had been committed in England.*" – see **[A1/Tab 4]**

the Respondents' Re-re-Amended Open Response[18]). The very purpose of s. 7 of the ISA is to provide for the granting of authorisations in respect of any act done outside the British Islands, where otherwise a person would be liable under the criminal or civil law of the UK. In addition, s. 7(9) of the ISA makes clear that such authorisations can relate to an act which is done in the British Islands, but which is or is intended to be done in relation to apparatus that is believed to be outside the British Islands.

21. In any event, it is not accepted that s. 31 of the CJA extends the scope of the territorial jurisdiction provisions in the CMA 1990 (see §37F of Privacy's Amended Grounds); nor are the broad assertions in §41B(b) of Privacy's Amended Grounds accepted as an accurate statement of the law[19].

22. **First** the CMA 1990 contains specific and express provisions as to what territorial links with the jurisdiction are and are not necessary in order for an offence (eg. under s.3) to be committed. It is made clear in s.4(1) that, for the purposes of any offence under s.3 of the CMA 1990, it is immaterial (a) whether the act or event, proof of which is required for conviction, occurred in England and Wales or (b) whether the accused was in England and Wales at the time. But, as made clear by s.4(2), at least one significant link with the jurisdiction must exist in the circumstances of the case for the offence under s.3 to be committed. Prior to 3 May 2015 a significant link was present if (a) the accused was in England and Wales at the time when he did the unauthorised act or caused it to be done or (b) the unauthorised act was done in relation to a computer in England/Wales (see s.5(3))[20]

23. In those circumstances the CMA 1990 is an example of a "*purely domestic regulation*" per Lord Parker CJ in *R v Naylor* [1962] 2 QB 527 i.e. it contains offences which are incapable of being committed where there are insufficient links with the jurisdiction and therefore are incapable of being transposed under the CJA 1948[21].

24. The same would also apply, for example, to RIPA 2000 **[A1/Tab 10]**. Section 1(1) of that Act creates an offence of unlawful interception of a communication being transmitted by a public postal service or a public

[18] At Open Bundle Part A p105
[19] See Open Bundle Part A at p19 and p21
[20] and changes to s.5 brought about in May 2015 now mean that, for a s.3 offence, a significant link can also be established if the accused was outside the UK at the time the act constituting the offence occurred and (a) the accused was a UK national at the time or (b) the act constituted an offence under the law of the country in which it occurred (see s. 5(1A)) [**A1/Tab 1]**.
[21] See also *Cox v Army Council* [1963] AC 48 where Lord Parker CJ, in the context of s.70 of the Army Act 1955 (which contains similar provisions to s.31 CJA 1948) made clear at §71 that there would be certain acts or omissions punishable if done in England which cannot be reproduced by any equivalent occurrence taking place outside the country.

telecommunications system. Section 1(2) sets out the circumstances in which the interception of a communication being transmitted by a private telecommunications system is an offence and, in each case, the interception must take place in the United Kingdom. The definitions of 'private telecommunications system' and 'public telecommunications system' require a link to the United Kingdom. Thus it would be impossible to transpose an interception on a foreign telecommunications system carried out by a Crown servant acting abroad. Moreover to criminalise a Crown Servant working abroad would place that Crown servant in a worse position than a Crown servant working in the United Kingdom and would therefore not operate fairly and within reasonable limits.

25. **Secondly**, even if the CJA 1948 did apply, the question whether there was any liability under s. 31 of that Act, read with the CMA 1990, would depend upon the specific circumstances in question including, *inter alia*, the answers to the following key questions:

(a) Whether the offence was contrary to the laws of the foreign country i.e. it would only be where the Crown Servant commits an offence contrary to the laws of the foreign country and which would be indictable in England, that section 31 of the CJA could apply. That follows from the fact that the section itself refers to the commission in a foreign country of an offence and avoids the absurdity of a Crown servant acting lawfully in the foreign country but exposing himself to criminal prosecution on return to England and Wales; and

(b) Whether the offence was committed in a "foreign country" which bears a special meaning derived from the British Nationality Act 1948, which was repealed in part and replaced with the British Nationality Act 1981 and which means that section 31 of the CJA does not apply to (a) Commonwealth countries, (b) the Republic of Ireland and (c) British overseas territories.

26. Thus, this matter is academic; in any event, the Claimants' contention that the CJA 1948 extends the scope of territorial jurisdiction of the CMA 1990 for Crown servants is wrong in law; but, even if it were right, the matter could only be determined on a case by case basis and is incapable of being addressed in the general terms contended for by the Claimants.

Issue 2: Does s.5 ISA 1994 permit the issue of a 'class' or 'thematic' warrant, i.e. a warrant authorising certain acts or types of acts in general rather than by reference to specified property or wireless telegraphy?

27. In §41C of Privacy's Amended Grounds it is asserted that s.5 ISA warrants,

unlike s.7 ISA authorisations, are incapable of being issued on a "class" or "thematic" basis because of the requirement that the action and the property both be "specified".

28. The genesis for this complaint appears to be the 2014 report of the Intelligence Services Commissioner, Sir Mark Waller dated 25 June 2015. When dealing with ISA property interference warrants **[Vol 1/CM1/p849ff]**, he stated as follows:

"• *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.

I accept the agencies' interpretation is very arguable. I also see in practical terms the national security requirement.

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. We remain in discussion to find a way to do so but I am anxious to ensure that they are not missing intelligence opportunities which might endanger national security.

I made five recommendations at each of the intelligence agencies and warrantry units in relation to what might be termed thematic property warrants:

> *1. For any warrants which might be considered to be thematic to be highlighted in the list provided for my selection;*
> *2. The terms of a warrant and the submission must always be such as to enable the Secretary of State to assess the necessity and proportionality;*
> *3. The assessment of proportionality and necessity should not be delegated;*
> *4. Property warrants should be as narrow as possible but circumstances where time constraints and national security dictate may allow a more broadly drawn "thematic" warrant; and*
> *5. As the agencies and the Secretaries of State have made clear to me is the case, thematic or broadly drawn warrants should not be asked for simply for administrative convenience.*

I have recommended in general, and not just for thematic warrants, that the submission attached to the warrant should set out all the limitations applied to the use of the warrant and particularly should identify what action is being taken to minimise intrusion into privacy." (see pages 18-19)

29. It is to be noted that the terms "*thematic*" and "*class*" as used by Privacy do not form part of the statutory requirements for the issue of a warrant under s.5. Insofar as the term "*thematic*" used by Privacy refers to the usage by the Commissioner the report set out above, the Respondents position is as follows:

30. **First** s.5(1) ISA provides: "*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*." That provision does not delimit the scope of a warrant to any single piece of property or single instance or method of entry on to or interference with property or wireless telegraphy.

31. **Secondly** by s.5(2) the Secretary of State may, on an application by GCHQ, issue a s.5 warrant authorising "*the taking, subject to subsection (3) …, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified*". Therefore if and insofar as action and/or property and/or wireless telegraphy is specified in a s.5 warrant, the warrant will be valid as regards that specification.

32. **Thirdly** whether action and/or any property and/or wireless telegraphy is "*specified*" in a warrant will depend upon the words used in the particular warrant. The phrase "*any property so specified*" in s.5(2) is not to be read as precluding the Secretary of State from issuing a warrant save in relation to a particular operation against a particular piece of property. Given the terms of

s.5 of the ISA "*property*" can be "*specified*" in a s. 5 warrant by description and such description may encompass more than one particular location or item of property eg. with reference to a described set of persons.

33. The Secretary of State can only sign a warrant if satisfied that the activity thereby authorised is necessary and proportionate in accordance with the statutory tests and that there are satisfactory arrangements in force with regard to the disclosure of information obtained under the warrant (see s.5(3)). In making that assessment the Secretary of State is required to consider whether what is sought to be achieved by the warrant could be achieved by other means (s.5(2A). As noted by the Commissioner there may be circumstances in which the requirements of national security mean that it is simply not possible to specify with precision a defined individual, as opposed to eg. a set of persons to which the warrant relates. But there is nothing in the language of the ISA which would preclude a warrant being issued on that basis provided the statutory tests are otherwise satisfied.

34. In those circumstances it is submitted that s.5 does permit a property to be specified in a warrant by description and it is not accepted that any warrants where this may have occurred were unlawful.

Issue 3: Does the power under s.5 ISA 1994 to authorise interference with "property" encompass physical property only, or does it also extend to intangible legal rights, such as copyright?

35. The only stated basis for the Claimants' contention that a warrant under section 5 ISA can pertain to interference with only physical property is that ss.5(3) and (3A) refer to interference with property "in the British Islands".[22] That reference is of no assistance:

(a) **First**, the natural reading of the phrase is that it is employed to distinguish between property in and outside the UK for the purposes of the scope of s.5 and not types of property: it is a phrase intended to limit the geographical scope of interference, not the type of property with which interference could occur.

(b) **Secondly**, if Parliament had intended to delineate different types of property and limit the scope of the term, it could have done so but chose not to.[23]

[22] Privacy Re-Amended Statement of Grounds §41D.
[23] In contrast, for example, the Criminal Damage Act 1971 is specifically limited to "tangible" property by s.10.

(c) **Thirdly**, the supposed tension between the use of the phrase "in the British Islands" and coverage of intangible property by section 5 is difficult to understand in circumstances where, in particular, copyright is a territorially delimited right in domestic law and, therefore, the reference is consistent with that limitation.[24]

(d) **Fourthly**, reading the term "property" as being qualified by the term "physical" would result in an anomalous position in practice on the Claimants' own case. The sort of interference contemplated by the Claimants ie. modification or adaptation of a computer programme on a target computer, would itself be *lawful* under a warrant: the reconfiguration of electrons on a computer so as to modify the manner in which it operated would be a physical interference which is contemplated to be permissible. The warrant would permit such action. Yet simultaneously, the Claimants also say that the very same rearrangement of electrons is also unlawful because it affects an intangible property right. There is no reason to suppose that Parliament intended such a state of affairs to be capable of arising when the overall purpose of the section is to enable lawful interference.

36. Thus the contention that s.5 warrants could not cover interferences with intangible property are unfounded.

37. But further and in any event, the Claimants fail to recognise that even if a s.5 warrant did not cover a potential inference with copyright, no basis for alleging any breach of copyright has been put forward:

(a) §41E of Privacy's Amended Grounds[25] is wholly vague as to the nature or type of the alleged interference with copyright and it is inadequately pleaded (by reference to other allegations made or otherwise).

(b) The Claimants purport to rely on EU Directive 2001/29 **[A1/Tab 14]** but its relevance is not understood. Notwithstanding that in their Amended Open Response of 25 September 2015 the Defendant explained that the relevant law of copyright is the domestic law of England and Wales and no breach thereof is alleged, no further explanation of the Claimants' position has been proffered. As made clear in the Open Response, it has not been contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law. It is noted that Directive 2001/29 was implemented in the United

[24] In particular Part I of the Copyright, Designs and Patents Act 1988 extends only to England and Wales, Scotland and Northern Ireland.
[25] See Open Bundle Part A/p22

Kingdom in particular in the Copyright Designs and Patents Act 1988 (as amended).

(c) Further or alternatively, insofar as it is relevant it is denied that:

i. the actions of the Defendant pursuant to the protection of national security interfere with any rights protected under Directive 2001/29; and/or

ii. any interference with such rights by the actions of the Defendants is unlawful or disproportionate.

38. The further references in §41F of Privacy's Amended Grounds do not assist the Claimants' case. The judgment Case C-293/12 *Digital Rights Ireland* **[A2/Tab 26]** was not concerned with copyright, did not consider standards required for derogations under Directive 2001/29 (albeit the relevance of which is not understood – see above) and did not purport to lay down "the standard required to justify a derogation from EU law rights" whether in relation to "surveillance" or otherwise. Indeed, it is noted that on 20 November 2015 the Court of Appeal gave a judgment in *Secretary of State for the Home Department* v *Davis & Watson* [2015] EWCA Civ 1185 in which it stated that its provisional view was that the judgment in *Digital Rights Ireland* did not lay down mandatory requirements even in relation to the matters with which it was directly concerned and ordered a preliminary reference to the CJEU in that regard.

39. Thus not only have the Claimants failed to make good their statutory interpretation contention, given the nature, scope and derogations available under copyright law they have failed to put forward any good basis for any breach of copyright.

ISSUES 4 AND 5 - ECHR

Is the regime which governs Computer Network Exploitation ("the regime") "in accordance with the law" under Article 8(2) ECHR / "prescribed by law" under Article 10(2) ECHR? In particular:

a. Is the regime sufficiently foreseeable?

b. Are there sufficient safeguards to protect against arbitrary conduct?

c. Is the regime proportionate?

d. Was this the case throughout the period commencing 1 August 2009?

Article 8 ECHR – the principles

40. As the Tribunal held at §37 of its judgment in *Liberty/Privacy* **[A2/Tab 22]**, in

order for an interference to be "*in accordance with the law*":

> "*i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action.*
>
> *ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an "adequate indication" given (Malone v UK [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable...*"

See also *Bykov v. Russia*, appl. no. 4378/02, 21 January 2009, at §78 **[A2/Tab 31]**, quoted at §37 of *Liberty/Privacy*.

41. As the Tribunal also noted in *Liberty/Privacy*, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §§38-40 and §137). See also in that respect, *Malone v UK* (1984) 7 EHRR14 at §§67-68m **[A2/Tab 42]**, *Leander v Sweden* [1987] 9 EHRR 433 at §51 **[A2/Tab 40]** and *Esbester v UK* [1994] 18 EHRR CD 72 **[A2/Tab 33]**, quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the *British Irish Rights Watch* case dated 9 December 2004 **[A2/Tab 21]** (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87): "*foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...*" (§38)

42. Thus, the national security context is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment **[A2/Tab 22]**). That is not least because the ECtHR has consistently recognised that the foreseeability requirement "*cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly*": *Malone v. UK*, §67 **[A2/Tab 42]**; *Leander v. Sweden*, §51 **[A2/Tab 40]**; and *Weber and Saravia v Germany* (2008) 46 EHRR SE5, §93 **[A2/Tab 49]**.

43. As to the procedures and safeguards which are applied, two points are to be noted.

44. **First** it is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* **[A2/Tab 42]** and §78 of *Bykov* **[A2/Tab 31]**; and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy* **[A2/Tab 22]**. Hence the reliance on the Code in *Kennedy v United Kingdom* [2011] 52

EHRR 4 at §156 **[A2/Tab 36]** and its anticipated approval in *Liberty v United Kingdom* [2009] 48 EHRR at §68 **[A2/Tab 41]** (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom* [1983] 5 EHRR 347).

45. **Secondly** it is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal concluded that it is "*not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise*" (§122), in order to satisfy the "in accordance with the law" requirement; and that the Tribunal could permissibly consider the "*below the waterline*" rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of *Liberty/Privacy*). At §129 of *Liberty/Privacy* the Tribunal stated:

> "*Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:*
>
> *i.* *The Code...itself refers to a number of arrangements not contained in the Code...*
>
> ii. *There is a system of oversight, which the ECHR has approved, which ensures that such arrangements are kept under constant review.*"

46. Those conclusions were reached in the context of the s. 8(4) RIPA interception regime. They are equally applicable to the equipment regime where the relevant Codes both refer expressly to undisclosed statutory "*arrangements*" under the ISA (see eg. §1.3 of the EI Code **[Vol 1/CM1/p707]** and §7.38 and §9.7 of the Property Code[26] **[Vol 1/CM1/p809/p815]**) and where there is similar oversight by the Intelligence Services Commissioner.

47. In the context of interception, the ECtHR has developed a set of minimum safeguards in order to avoid abuses of power. These are referred to as 'the *Weber* requirements'. At §95 of *Weber* **[A2/Tab 49]**, the ECtHR stated:

> "*In its case-law on secret measures of surveillance, the Court 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.*" (numbered items added for convenience, see §33 of *Liberty/Privacy*)

[26] And see §2.19 of the 2002 version of the Property Code.

(And see also *Valenzuela Contreras v Spain* (1999) 28 EHRR at §59)

48. However it is important to recognise what underpins the *Weber* requirements, as highlighted at §119 of the *Liberty/Privacy* judgment. In particular, §106 of *Weber* states as follows:

> "*The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life,* ***it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security*** *(see, inter alia, Klass and Others, cited above, p. 23, § 49; Leander, cited above, p. 25, § 59; and Malone, cited above, pp. 36-37, § 81).* ***Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse*** *(see Klass and Others, cited above, pp. 23-24, §§ 49-50; Leander, cited above, p. 25, § 60; Camenzind v. Switzerland, judgment of 16 December 1997, Reports 1997-VIII, pp. 2893-94, § 45; and Lambert, cited above, p. 2240, § 31).* ***This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law*** *(see Klass and Others, cited above, pp. 23-24, § 50).*" (emphasis added)

49. This emphasis on the need to consider all the circumstances of the case was recently reiterated by the ECtHR in *RE v United Kingdom* (Application No. 62498/11) 27 October 2015 at §127 **[A2/Tab 44]**. In that case, because of the "*extremely high degree of intrusion*" involved in the surveillance of legal consultations it expected the same safeguards to be in place as in an interception case, at least insofar as those principles could be applied to the surveillance in question (see §131). On the specific facts of that case, a breach of Article 8(2) ECHR was found given that the surveillance regime as it applied to legal consultations did not contain sufficient provisions as regards the examination, use and storage of the material obtained and the precautions to be taken when communicating the material to other parties or erasing/destroying the material (see §§138-141). The ECtHR contrasted the provisions in Part I of RIPA and the Interception Code, which the Court approved in *Kennedy*, and concluded that they provided an example of the type of provisions which were required in this context.

50. The Tribunal in *Liberty/Privacy* placed considerable reliance on **oversight mechanisms** in reaching their conclusion that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8 compliant. In particular:

(a) The role of the Commissioner and "*his clearly independent and fully implemented powers of oversight and supervision*" have been long recognised by the ECtHR, as is evident from *Kennedy* at §§57-74, 166, 168-169 **[A2/Tab 36]** (see *Liberty/Privacy* at §§91-92 **[A2/Tab 22]**). Whilst the Tribunal will, of course, form its own judgment about the effectiveness of his supervision in the CNE context, it is clear that this is potentially a very important general safeguard against abuse. In *Liberty/Privacy* the Tribunal relied, in particular, on his duty to keep under review the adequacy of the arrangements required by statute and by the Code, together with his duty to make a report to the Prime Minister if at any time it appeared to him that the arrangements were inadequate.

(b) The advantages of the Tribunal as an oversight mechanism were emphasised at §§45-46 of *Liberty/Privacy*, including the "*very distinct advantages*" over both the Commissioner and the ISC for the reasons given at §46 of the judgment.

(c) In addition the ISC was described as "*robustly independent and now fortified by the provisions of the JSA*" (see §121 of *Liberty/Privacy*) and therefore constituted another important plank in the oversight arrangements.

51. Consequently there is a need to look at all the circumstances of the case and the central question under Art. 8(2) is whether there are:

> "*...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.*" (see §125 of the *Liberty/Privacy* judgment)

Application of those legal tests to the Equipment Interference Regime

Preliminary matters

52. Prior to considering the detailed safeguards which apply to the Equipment Interference regime, the Respondents make three preliminary points.

53. **First**, it is not accepted, even on the basis of the factual assertions made in the Claimants' Grounds (which are neither confirmed nor denied), that such activities are factually or legally more intrusive than other forms of surveillance or data-gathering, including the interception of communications (see §§42-46 of the Privacy Grounds and §§55-57 of the Greennet Grounds).

54. As stated at §42-44 of Ciaran Martin's first witness statement **[Open Bundle, Part B/p124ff]**, whilst it is accepted that CNE operations can be highly intrusive, they are not in general more intrusive than other operations conducted by GCHQ eg. under RIPA 2000 or the ISA. For example Part II of RIPA permits public authorities to engage in intrusive surveillance. A listening device directed at say a bedroom clearly has the potential to obtain information of an extremely private and personal data. In addition with the advent of certain types of remote storage, much of the material referred to in the Claimants' complaints could potentially be available via interception under Part I of RIPA.

55. The ECtHR has expressly referred to the fact that "*rather strict standards*" apply in the interception context, but do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* (2011) 53 EHRR 24, at §66 **[A2/Tab 48]** and see also *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, *per* Lord Carswell at §85 **[A2/Tab 24]**. In *RE v United Kingdom* the ECtHR held that an "*extremely high degree of intrusion*" involved in the surveillance of legal consultations meant that the same safeguards had to be in place as in the interception context.

56. Here there is no factual or legal justification for asserting that an even stricter set of standards ought to apply to equipment interference activities, over and above those which would apply eg. in an interception case.

57. Therefore in circumstances where GCHQ accepts that these activities represent a similar level of intrusiveness in Article 8 ECHR terms to eg. interception under Part I of RIPA, it is acknowledged that consideration of the *Weber* requirements is necessary as part of an assessment of all the circumstances of the case.

58. **Secondly**, as has already been made clear, GCHQ does not seek to carry out indiscriminate mass surveillance activities of the sort alleged by the Claimants both in the Grounds and in their witness evidence (see §36 of Ciaran Martin's first statement **[Open Bundle Part B/p131-132]** and see also §7 of his third statement dated 24 November 2015). Such activities are precluded by the clear statutory framework which regulates GCHQ's activities. CNE activities must be authorised by the Secretary of State and are subject to strict tests of necessity and proportionality and legitimate aim as set out in the ISA. These authorisations and the internal processes which are in place to manage these activities are subject to independent scrutiny by the Intelligence Services Commissioner and the ISC.

59. It follows from this that many of the examples given in the Claimants'

evidence about the possibilities created by CNE techniques bear no relation to the reality of GCHQ's activity and/or would be unlawful having regard to the relevant statutory regime.

60. It also follows that the Tribunal must exercise caution when approaching the assumed facts for the purposes of testing the legal issues. For very good reason GCHQ is unable to confirm or deny what particular CNE techniques/capabilities it has or what type of CNE operations are conducted by it. It has therefore been extremely difficult for GCHQ to engage in OPEN with the assumed facts without breaching NCND (although it has sought to do so in its CLOSED evidence).

(a) For example §6(e) refers to "*the use of CNE in respect of numerous devices, servers or networks without first having identified any particular device or person as being of intelligence interest*". If that were taken literally it might suggest that GCHQ would engage in CNE activities on a speculative/trawling basis, without any proper justification. But that would clearly be precluded by the legislation and the core requirements of necessity and proportionality. Consequently it is only having considered the CLOSED evidence about GCHQ's actual activities that the Tribunal can properly assess whether the activities are met with adequate safeguards and are proportionate.

(b) Similarly §6(d) of the assumed facts refers to "*the use of CNE in such a way that it creates a potential security vulnerability in software or hardware, on a server or a network*". Here GCHQ can respond (at least in general terms) and has made clear in Mr Martin's first statement that operations are carried out in such a way as to minimise that risk (see §41 **[Open Bundle, Part B/p132-133]**). To leave targets open to exploitation by others would increase the risk that privacy would be unnecessarily intruded upon and would also increase the risk of GCHQ's sensitive tools and techniques being identified. Consequently GCHQ does not intrude into privacy any more than is necessary to carry out its functions and takes steps to to minimise these risks. It also carries out important internet safety and cyber-security activities, including detecting and disclosing security vulnerabilities, as explained in §§40-41 of Mr Martin's first statement **[Open Bundle, Part B/p132-133]**. Consequently the reality of GCHQ's activities is inadequately reflected in a bald statement that CNE may be used in such a way that it creates potential security vulnerabilities in software or hardware or a server/network.

(c) In addition §6(b) refers to the "*creation, modification or deletion of*

information on a device, server or network". In that regard whilst GCHQ recognises that CNE activity could theoretically change the material on a computer eg. by the installation of an implant which would itself amount to a change, it would be neither necessary nor proportionate, nor operationally sensible, to make more than the most minimal and to the greatest extent possible, transient, changes to targeted devices (see §46 of Mr Martin's first statement **[Open Bundle, Part B/p133]**.). Consequently the extent to which a CNE operation involves the creation, modification or deletion of information would always have to be part of the necessity and proportionality justification.

61. **Thirdly**, contrary to the assertion made in the Claimants' Grounds, there is a clear legal framework governing any equipment interference activities, as set out in detail earlier in this Response. The availability of warrants under s. 5 and authorisations under s. 7 of the ISA, do provide a firm legal framework which is supplemented in important respects by the CMA, HRA, the DPA, the OSA, the relevant Codes and GCHQ's internal arrangements. That statutory scheme, in common with the interception regime in RIPA, makes certain activities an offence (as is the case eg. in s. 1 of RIPA which makes it an offence, without lawful authority to intercept certain communications) but is coupled with a regime for the issuing of warrants/authorisations which render the activity lawful if strict conditions are satisfied. The suggestion that the availability of a warrant under the ISA "*simply cancels any unlawfulness*" is a misrepresentation and an over-simplification of the statutory scheme and the safeguards which are inherent within it.

62. The Equipment Interference regime is therefore "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation and in relevant Codes and also in relevant internal arrangements/safeguards which are applied by GCHQ. The Claimants' argument that there is no relevant legal regime that regulates the circumstances in which and the conditions in which GCHQ may interfere with equipment is therefore untenable.

Compatibility of the regime since February 2015

Weber (1) and (2)

63. As noted by the Tribunal at §115 of *Liberty/Privacy* **[A2/Tab 22]**, *Weber* (1) and (2) overlap and therefore can be taken together.

64. These requirements i.e. the "offences" which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read, in particular, with §1.6,

Chapter 2, Chapter 4 and §7.7-§7.8 of the EI Code **[Vol 1/CM1/p704ff]**.

65. As noted in *RE v United Kingdom* **[A2/Tab 44]**, although sufficient detail should be provided of the nature of the offences in question, the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to the activity (see §132). Consequently terms such as "*national security*" and "*serious crime*"[27] are sufficient (see *RE* at §133 and §116 of the *Liberty/Privacy* judgment **[A2/Tab 22]**). In addition it was also accepted in *RE* that it may not be necessary to know in advance precisely what individuals will be affected eg. by the surveillance measures in each case. Nevertheless given that the application was required to set out in full the information that was known and the proportionality of the measure was subsequently scrutinised in detail, no further clarification of the persons liable to be subject to the measures could reasonably be required (see §136).

66. As to the procedures for authorising CNE activities, these are addressed specifically at Chapter 4 of the EI Code **[Vol 1/CM1/p719ff]**. In particular, at §4.6 a detailed set of criteria are identified in terms of the information which is provided to the Secretary of State when applying for the issue or renewal of a s.5 warrant and this information must also be provided, where reasonably practicable, for any section 7 authorisation (see §7.7 and §7.2 of the EI Code **[Vol 1/CM1/p726-727]**). That paragraph states:

"*4.6 An application for the issue or renewal of a section 5 warrant is made to the Secretary of State. Each application should contain the following information:*

- *the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;*
- *sufficient information to identify the equipment which will be affected by the interference;*
- *the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;*
- *what the operation is expected to deliver and why it could not be obtained by other less intrusive means;*
- *details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.*
- *whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;*
- *details of any offence suspected or committed where relevant;*
- *how the authorisation criteria (as set out at paragraph 4.7 below) are met;*
- *what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);*
- *where an application is urgent, the supporting justification;*

[27] as found in the ISA (see, for GCHQ, s5(3) and s.7(3) of the ISA read with s.3(2).

- *any action which may be necessary to install, modify or remove software on the equipment;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.*"

It is to be noted that a similar provision to §4.6 above (i.e. §5.2 of the Interception Code) was described in *Liberty/Privacy* as "*impressive*" at §116(iv) **[A2/Tab 22]**.

67. In addition, §4.7 contains a checklist of matters about which the Secretary of State must be satisfied/consider before issuing a warrant/authorisation including:

(a) being satisfied that it is necessary for the purposes of carrying out the intelligence services functions;
(b) being satisfied that it is proportionate;
(c) taking into account whether there are other means by which the information could reasonably be obtained; and
(d) being satisfied that there are satisfactory arrangements in place as regards disclosure of any information obtained.

68. These provisions are also accompanied by detailed guidance in Chapter 2 of the Code **[Vol 1/CM1/p711]** on the requirements of necessity and proportionality in this context, including issues such as collateral intrusion and the need to consider less intrusive alternatives. General best practice guidance is also given at §§2.16 and 2.17 including making sure that there is a designated senior official within each of the Intelligence Services responsible for, inter alia, the integrity of the process to authorise equipment interference and engagement with the Commissioner.

69. More specifically, in terms of the procedures for s.7 authorisations:

(a) As noted above, the same procedures and safeguards apply as under s.5 ISA (§7.2 EI Code **[Vol 1/CM1/p726]**), including the detailed authorisation procedures in Chapter 4. In particular any application for a s.7 authorisation to the Secretary of State should contain the same information, as far as reasonably practicable in the circumstances, as an application for a s.5 warrant (§7.6 EI Code **[Vol 1/CM1/p726-727]**).

(b) Once a s.7 authorisation has been made by the Secretary of State, which may be specific to a particular operation or user or may relate to a broader class of operations (§7.6 EI Code **Vol 1/CM1/p726-727]**), the Code makes clear that it is necessary for internal approval to

conduct operations under that authorisation to be sought from a designated senior official.

(c) In circumstances where the equipment interference is likely or intended to result in the acquisition of confidential information, authorisation should be sought from an Annex A approving officer, which in GCHQ's case is a Director of GCHQ (see §7.12 EI Code **Vol 1/CM1/p727]**).

(d) Clear guidance is provided as to what information should be included in any application for an internal approval at §7.13 of the EI Code [**Vol 1/CM1/p728]** which essentially replicates and requires the same information as any application to the Secretary of State for a s.5 warrant. It states:

> *"The application for approval must [should[28]] set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must [should[29]] be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations."*

As is evident from this final part of §7.13, there is specific provision for the FCO to be consulted, or the endorsement of the Secretary of State obtained for particularly sensitive operations.

70. It is therefore submitted that the regime is sufficiently clear both as to the nature of the offences which may give rise to equipment interference activity and the categories of person liable to be subject to such measures.

71. It is also to be noted, in terms of substantive safeguards, that there are additional layers of assurance built into the s.7 approvals process including:

(a) An increasing emphasis on providing detailed information to the Secretary of State about the type of CNE activities covered by s.7 class authorisations. For example since July 2014 GCHQ has copied to the

[28] "*should*" now appears in the November 2015 version of the Code

[29] Ibid

FCO all of its internal s.7 approvals for CNE operations which were given pursuant to the class authorisation and serious attention is given to this by senior Ministers and their advisors including, *inter alia*, meetings to discuss individual warrants/authorisations (see §63 of Ciaran Martin's first statement [**Open Bundle/Part B/p138]** and §§9-11 of his third statement).

(b) Within GCHQ there is an internal specialist risk assessment panel, involving a range of relevant technical, operational and policy leads, which provides expert oversight and assurance that the tools and techniques being used and the way in which they are used, present an acceptable level of technical and operational risk. This includes providing an audit trail and a 'history' of decisions which for example are used to inform risk assessment statements in s.7 approval requests and political decisions (see §65 of Ciaran Martin's first witness statement).

(c) In accordance with §7.13 of the EI Code discussed above [**Vol 1/CM1/p728]**, if an operation is judged to present a significant risk, the proposal will be submitted to FCO officials or the Secretary of State and GCHQ will also seek FCO legal advice if a proposed operation involves issues of international law (see §66 of Ciaran Martin's first witness statement [**Open Bundle/Part B/p138]**).

***Weber* (3)-(6)**

72. The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are dealt with in the combination of the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 2, 4, 6 and 7 of the EI Code and GCHQ's internal arrangements.

73. As to **duration**:

(a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled – see s.6 and ss.7(5)-7(7) of the ISA (at **[A1/Tab 7]** and referred to at §§23-26 and §§33-35 of the Appendix to this skeleton).

(b) In addition the EI Code contains important provisions on reviewing warrants and the frequency of reviews, which apply equally to s.7 activity (see §§2.13-2.15 and §7.2 [**Vol 1/CM1/p712/p726]**) and for renewals and cancellations of s.5 warrants (see §§4.10-4.13 [**Vol 1/CM1/p721]**) and for renewals of s.7 authorisations (see §§7.15-7.16

[**Vol 1/CM1/p728]**). It is to be noted that in *RE v United Kingdom* similar provisions in Part II of RIPA and in the revised Property Code were considered to be "sufficiently clear" see §137 **[A2/Tab 44]**.

(c) In addition, in terms of the s.7 internal approvals process, the EI Code makes specific provision for regular reviews to ensure that operations continue to be necessary and proportionate. At §7.14 it states [**Vol 1/CM1/p728]**:

> *"All internal approvals must [should[30]] be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."*

74. In addition there are detailed safeguards which apply which mirror the safeguards in s.15 of RIPA in the interception regime, as regards the **handling, dissemination, copying, storage, disclosure and security arrangements** for information obtained as a result of equipment interference.

(a) These include detailed safeguards in Chapter 6 of the EI Code (see the Appendix to this skeleton at §62ff and **Vol 1/CM1/p723-725**) which include, *inter alia*, provisions which:

i. limit the number of persons to whom any information is disclosed to the minimum necessary for the proper discharge of the Intelligence Services functions, including applying the 'need to know' principle (EI Code §§6.6-6.7);
ii. limit the circumstances in which information obtained by equipment interference can be copied (EI Code §6.8);
iii. require information obtained by equipment interference to be handled and stored securely and inaccessible to persons without the required level of security clearance (EI Code §6.9 and §6.11);

(b) Further GCHQ must ensure that there are internal arrangements in force, which are approved by the Secretary of State, for securing that the requirements set out in Chapter 6 of the EI Code are satisfied in relation to all information obtained by equipment interference (see §6.4 of the EI Code) and these internal arrangements should be made available to the Commissioner (see §6.5 of the EI Code).

[30] Ibid

(c) Any information emanating from equipment interference can be used by GCHQ only in accordance with s.19(2) of the CTA as read with the statutory definition of GCHQ's functions (in s. 3 of the ISA) and only insofar as that is proportionate under s.6(1) of the HRA (see the Appendix to this skeleton at §§8-10 and §§101-104).

(d) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the seventh data protection principle, which provides:

> *7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."[31]

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question (see the Appendix to this skeleton at §§106-108).

(e) Any disclosure eg. deliberately in breach of the "*arrangements*" for which provision is made in s.4(2)(a) of the ISA would be a criminal offence under s.1(1) of the OSA which could attract imprisonment of up to two years (see the Appendix to this skeleton at §109) .

(f) Further a member of the intelligence service will commit an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the ISA read with s.1(1)). Conviction may lead to imprisonment of up to 3 months. Consequently this statutory obligation is relevant to the publicly available safeguards for the handling and security arrangements for information obtained through equipment interference (see the Appendix to this skeleton at §110).

(g) Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 at §§191-194).

[31] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

(h) Finally any disclosure of such information must satisfy the constraints imposed in ss. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

75. In addition the EI Code contains important **record keeping** obligations which are relevant to the processes for handling this material. At Chapter 5 of the EI Code [**Vol 1/CM1/p722]** there is a checklist of matters which should be centrally retrievable for at least 3 years – as set out at §§60-61 of the Appendix to this skeleton argument.

76. As to **destruction**:

(a) Chapter 6 of the EI Code [**Vol 1/CM1/p723-725]** contains provisions about destruction at §6.10 including that information obtained by equipment interference and all copies, extracts and summaries thereof, be marked for deletion and securely destroyed as soon as they are no longer needed to fulfil the Intelligence Services functions. Further if such information is retained it should be reviewed at appropriate intervals to confirm if the justification for its retention is still valid.

(b) In any event, pursuant the DPA, GCHQ is not exempt from an obligation to comply with the fifth data protection principle, which provides:

> "*5. Personal data processed*[32] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …"*

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being used/retained (see the Appendix to this skeleton at §§106-108).

77. In those circumstances, Weber requirements (3)-(6) are also met.

78. It is also to be noted, in terms of substantive safeguards, that GCHQ has a comprehensive programme of training and testing in place for those involved in CNE operations and for intelligence analysts who may have access to data obtained in CNE operations. This training includes operational and mandatory

[32] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

legalities training and the training involves testing and regular re-assessment (see §68C of Ciaran Martin's first witness statement **[Open Bundle/Part B/p139]**).

79. As set out above, when assessing whether there are adequate arrangements in place to give the individual adequate protection against arbitrary interference, both the (1) below the waterline arrangements and (2) oversight mechanisms in the regime are also relevant to the question of Article 8 compliance.

80. The **below the waterline** rules, requirements and arrangements can be appropriately assessed by the Tribunal in CLOSED based on the CLOSED evidence which has been served by the Respondents. It is of note however that, as a result of the disclosure process in these proceedings, some details about these arrangements are now in OPEN, as set out at §§99B-99ZS of the Re-Re-Amended OPEN response and as replicated in §138ff of the Appendix to this skeleton argument. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime. Of particular note is the following:

(a) The provision of internal guidance in the form of the Compliance Guide and both s.5 and s.7 ISA Guidance on the processes for applying, renewing and cancelling warrants/authorisations.
(b) Internal safeguards which ensure that decisions to obtain data from implanted devices are lawful, including the provision of training and legal advice.
(c) Internal policies for the storage of and access to data, including the setting of maximum limits for storage of operational data. In this regard it is to be noted that all operational data, including that obtained by CNE, is treated as if it was obtained under RIPA.
(d) Internal rules regarding the handling/disclosure/sharing of operational data, again which apply as if the material had been obtained under RIPA.
(e) Detailed record-keeping arrangements, including processes for keeping all internal Approvals and Additions (see §86B and §71L of Ciaran Martin's first witness statement).

81. As to the **oversight mechanisms** which are relevant to the Article 8(2) compatibility of the regime, the extent of scrutiny of GCHQ's s.5/s.7 ISA operations in this area is of some considerable importance.

82. As is evident from the first witness statement of Ciaran Martin at §§69-73 **[Open Bundle/Part B/pp140-144]** the **Commissioner** plays a very important role in scrutinising the CNE operations of GCHQ. During his visits (both formal and 'under the bonnet') it is apparent that there is a constructive

dialogue between GCHQ and the Commissioner about CNE activities, their authorisation processes and the safeguards which apply to them. These visits have included paying particular attention to the "Additions" layer (under internal approvals) of the s.7 authorisation process and GCHQ's operational use of CNE (see §§71I-71K of Ciaran Martin's first statement).

83. Of particular importance are the Commissioner's conclusions in his 2014 report about GCHQ's record keeping and its s.7 internal approvals process. In particular in his 2014 report he stated:

> "*GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips.*" *...*
>
> "*My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration that was given to each operation; it was clear to me that a great deal of thought was going into the process…" ...*
>
> *... "I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion."*
>
> *"I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I recommended that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ*."

These comments endorse the care and attention which is being given within GCHQ to these processes and the effectiveness of the protections which guard against arbitrary conduct.

84. The **ISC** specifically considered GCHQ's equipment interference activities as part of its review "*Privacy and Security: A modern and transparent legal framework*" published on 12 March 2015 **[Vol 1/CM1/p555ff]**. That report, as the Committee made clear in paragraph (v) of the introduction, contained an unprecedented amount of information about the intrusive capabilities used by the UK SIAs. Overall the Committee concluded that the UK SIAs do not seek to circumvent the law, including the requirements of the HRA which governs everything the Agencies do (p2). As is evident from §173-178 of the report this included scrutiny of GCHQ's computer network activities[33] **[p621-624]**.

[33] In terms of the concerns expressed at §177 of the ISC report, the evidence of Ciaran Martin at §71L of his first statement is to be noted i.e. given the Commissioner's clear endorsement of GCHQ's

85. It is submitted that the combination of these oversight mechanisms, including the important oversight provided by this Tribunal, are important safeguards in the context of the Art 8(2) compatibility of the regime.

86. **In conclusion** since February 2015 the Equipment Interference Regime has been sufficiently accessible and "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2). Article 10 adds nothing to the analysis under Article 8 ECHR – see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 **[A2/Tab 49]** and see also §12 and §149 of the *Liberty/Privacy* judgment **[A2/Tab 22]**.

Compatibility of the regime pre February-2015

87. When considering the compatibility of the regime pre-February 2015 the relevant Code of Practice is the Covert Surveillance and Property Interference Code ("the Property Code") as addressed in detail at §§76-100 of the Appendix to this skeleton argument. This was first issued in 2002 (called the Covert Surveillance Code of Practice) and was then revised in September 2010 with further revisions in 2014. As explained in the Appendix to this skeleton, there were no material differences between the 2010 and 2014 versions of the Property Code in terms of property interference.

Weber (1) and (2)

88. The Respondent repeats those submissions at §§63-65 above regarding these requirements. These requirements i.e. the "offences" which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read, in particular, with Chapter 3 and 7 of the 2010/2014 Property Code and Chapter 2 and 6 of the 2002 Property Code.

89. In the 2010/2014 version of the Property Code **[Vol 1/CM1/p734ff]**:

    (a) Chapter 7 set out the authorisation processes for property interference including a checklist of matters about which the Secretary of State had to be satisfied/consider before issuing a warrant/authorisation including at §7.38 **[p809]**:

        i. being satisfied that it is necessary for the purposes of carrying out the intelligence services functions;

---

internal record keeping, including its s.7 processes, he does not consider that the statement relates to GCHQ's s.7 ISA operations.

ii. being satisfied that it is proportionate;

iii. taking into account whether there are other means by which the information could reasonably be obtained; and

iv. being satisfied that there are satisfactory arrangements in place as regards disclosure of any information obtained.

(b) In addition it was made clear in §7.37 **[p809]** that the intelligence services should provide the same information as other agencies, as and where appropriate, when making applications for the grant or renewal of property warrants. That in turn meant that the checklist at §7.18 **[p804]** setting out the information which should be specified in applications should be provided where possible i.e.

- "*the identity or identities, where known, of those who possess the property that is to be subject to the interference;*

• sufficient information to identify the property which the entry or interference with will affect;

• the nature and extent of the proposed interference;

• the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;

- *details of the offence suspected or committed;*

• how the authorisation criteria (as set out above) have been met;

• any action which may be necessary to maintain any equipment, including replacing it;

• any action which may be necessary to retrieve any equipment;

• in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and

• whether an authorisation was given or refused, by whom and the time and date on which this happened."

(c) Chapter 3 set out general rules on authorisations, including guidance on the requirements of proportionality at §§3.3-3.6 including specific elements of proportionality that should be considered at §3.6 (see §80 of the Appendix to this skeleton argument and **[Vol 1/CM1/p760]**);

(d) Guidance on collateral intrusion was also given in that Chapter at §§3.8-3.11 (see §83 of the Appendix **[Vol 1/CM1/p761-762]**);

(e) Best working practice guidance was also given at §§3.27-3.28 (**[Vol 1/CM1/p766-767]** NB. §§3.28-3.29 in the 2014 version) including making sure that there is a designated senior official within each of the Intelligence Services responsible for, *inter alia*, the integrity of the process to authorise equipment interference and engagement with the Commissioner.

90. In the 2002 Property Code similar provisions were to be found, in particular, in Chapter 2 and Chapter 6 – see §§93-99 of the Appendix to this skeleton argument, including an alternative version of the checklist of information to be

specified in applications at §6.12 of the Code.

91. In the light of the matters set out above it is submitted that the pre-February 2015 regime is sufficiently clear both as to the nature of the offences which may give rise to equipment interference activity and the categories of person liable to be subject to such measures.

Weber (3)-(6)

92. The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 7-9 of the 2010/2014 Property Code and Chapter 6 of the 2002 Property Code and GCHQ's internal arrangements. In particular:

93. In terms of **duration**:

(a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled – see s.6 and s.7(5)-7(7) of the ISA (referred to at §23-26 and 33-35 of the Appendix to this skeleton, **[A1/Tab 7]**).

(b) In addition the Property Code contains important provisions on renewals and cancellations:

i. In the 2010/2014 Property Code these are contained in §§7.39-7.42 (see §86 of the Appendix to this skeleton and **[Vol 1/CM1/p810]**); and

ii. In the 2002 Property Code these are contained in §§6.34-6.35 (see §97 of the Appendix).

It is to be noted that in *RE v United Kingdom* the provisions in Part II of RIPA and in the Revised Property Code (i.e. issued in 2010) were considered to be "sufficiently clear" see §137 **[A2/Tab 44]**.

94. As regards the **handling, dissemination, copying, storage, disclosure and security arrangements** for information obtained as a result of equipment interference.

(a) Pursuant to the 2010/2014 Property Code, guidance is given as to the handling of material obtained through property interference. §9.3 of the Code **[Vol 1/CM1/p814]** addresses the retention and destruction of material and stated as follows:

> "*Each public authority must ensure that arrangements are in place for the* ***secure handling, storage and destruction of material*** *obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller,* ***must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998*** *and any relevant codes of practice produced by individual authorities relating to the* ***handling and storage of material***." (emphasis added)

In addition the Code states at §9.7 **[p815]** that, in relation to the Intelligence Services:

> "***The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the ... 1994 Act***." (emphasis added)

In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

(b) Any information emanating from equipment interference can be used by GCHQ only in accordance with s.19(2) of the CTA as read with the statutory definition of GCHQ's functions (in s. 3 of the ISA) and only insofar as proportionate under s.6(1) of the HRA.

(c) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the seventh data protection principle, which provides:

> *" Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."[34]

Accordingly, as set out earlier in these submissions, if GCHQ obtain any information as a result of any property interference which amounted to personal data, it is obliged to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question (see the Appendix to this skeleton at §§106-108.

(d) Any disclosure eg. deliberately in breach of the "arrangements" for which provision is made in s.4(2)(a) of the ISA would be a criminal

[34] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

offence under s.1(1) of the OSA which could attract imprisonment of up to two years (see the Appendix to this skeleton at §109).

(e) Further a member of the intelligence service will commit an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the ISA read with s.1(1)). Conviction may lead to imprisonment of up to 3 months (see the Appendix to this skeleton at §110).

(f) Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 at §§191-194).

(g) Finally any disclosure of such information had to satisfy the constraints imposed in s. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

95. As to **destruction**:

(a) The 2010/2014 Property Code address the destruction of material at §9.3 [**Vol 1/CM1/p814]** and states as follows :

> "*Each public authority must ensure that arrangements are in place for the secure handling, storage and* ***destruction*** *of material obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.*" (emphasis added)

In addition the Code states at §9.7 **[p815]** that, in relation to the Intelligence Services:

> "***The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions…"*** (emphasis added)

(b) In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

(c) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the fifth data protection principle, which provides:

> "*Personal data processed*[35] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …"*

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained/used (see the Appendix to this skeleton at §§106-108) .

96. In those circumstances, the *Weber* requirements (3)-(6) are also met for the pre-February 2015 regime.

97. In addition, those substantive safeguards set out at 78 to 85 above including the below the waterline arrangements and the oversight mechanisms, are highly relevant to the Article 8 compatibility of the pre-February 2015 regime. Those submissions are not repeated, but are of relevance when considering "all the circumstances" and whether overall the pre-February 2015 regime contained effective safeguards against abuse.

98. Whilst it is accepted that pre-February 2015 regime does not contain some of the detail to be found in the EI Code (eg. in Chapter 6), it is submitted that, in all the circumstances of the case, and particularly given the safeguards and the supervision regime which were in place throughout, it was "in accordance with the law" pursuant to Article 8 ECHR.

Proportionality

99. For reasons discussed earlier in this skeleton argument, there are considerable limits on GCHQ's ability to address in OPEN the matters which are relevant to an assessment of the proportionality of GCHQ's activities. However the following brief OPEN submissions are made at this stage:

(a) As made clear eg. in *Leander v Sweden*, in the field of national security the state has a wide margin of appreciation in assessing the pressing social need and in choosing the means for achieving the legitimate aim of protecting national security (see **A2/Tab 40**/§§58-59 and see also the Tribunal's conclusions in *Liberty/Privacy* at §§38-39 **[A2/Tab**

[35] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

22]).

(b) As explained in Ciaran Martin's first witness statement at §§6-20 and 28-34 **[Open Bundle/Part B/pp125-129, 130-131]** the terrorist threat currently facing the UK is SEVERE and GCHQ's CNE activity is increasingly required to enable the UK to counter that threat. The fact that CNE may, in some cases, be the only way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country is of obvious importance to the proportionality assessment (see §31 of Ciaran Martin's first statement).

(c) As already made clear, the Claimants' extreme allegations about the size, scope and intrusiveness of GCHQ's CNE activity must be contrasted with the reality of GCHQ's operations, as have been explained in detail in the CLOSED evidence.

100. It is therefore submitted that GCHQ's CNE activities are proportionate and have been throughout the relevant period since 1 August 2009.

Specific questions posed in the list of issues

101. A number of specific questions have been posed in the list of issues at §5. Some of the answers to these questions follow from and are answered by the submissions above. However, in summary, the Respondents' answers to these questions is as follows:

a. Should CNE activities be authorised by specific and individual warrants, or is it sufficient that they be authorised by 'class' or 'thematic' warrants or authorisations without reference to a specific individual target?

102. Section 5 ISA activity is authorised by specific warrants and submissions about the compatibility of descriptive warrants with s.5 ISA have already been addressed under Issue 2 above.

103. Section 7 authorisations can relate to a broader class of operations, as made clear in s.7 of the ISA and at §7.6 of the EI Code. Further there is nothing in the case law under Article 8 ECHR which precludes this, particularly given that the regime satisfies the minimum *Weber* requirements for the reasons set out in detail above.

104. In this regard it is relevant that *Weber* itself concerned a regime known as "strategic monitoring" which did not involve interception that had to be targeted at a specific individual or premises (see §§110-111 **[A2/Tab 49]**). Despite that, the applicants' Art. 8 challenge in *Weber* to strategic monitoring

was not merely rejected, it was found to be "*manifestly ill-founded*" (§§137-138) and thus inadmissible. In the s.7 ISA context, whilst the authorisation may relate to a broad class of operations and may not be narrowed to a specific target in the first instance, there are then detailed procedures in place, both above and below the waterline, to ensure that operations pursuant to that authorisation meet the same stringent tests as would be required for a s.5 ISA warrant (see §7.13 of the EI Code **[Vol 1/CM1/p728]**).

105. Consequently the procedures for s.7 authorisations are entirely compatible with Article 8 ECHR.

b. What records ought to be kept of CNE activity? Is it necessary that records of CNE activity are kept that record the extent of the specific activity and the specific justification for that activity on grounds of necessity and proportionality, identifying and justifying the intrusive conduct taking place?

106. The EI Code makes provision for the records which should be kept of CNE activity (see Chapter 5 of the EI Code **[Vol 1/CM1/p722]**). In addition GCHQ's own processes include maintaining indefinitely records of the application for, renewal of, approval of and cancellation of all warrants under s.5 and class authorisations and internal approvals under s.7. These include comments or stipulations from the Secretary of State relating to them (see §68B of Ciaran Martin's first statement **[Open Bundle/Part B/p139]**). By definition, that means that the specific justification for the activity in question in terms of necessity and proportionality will be included as part of the record keeping.

107. The Respondents accept that such records should be kept and would emphasise the extent to which the Commissioner has commended GCHQ's compliance in this regard; stating in his 2014 report:

> "*GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips.*" ...
>
> *"I was impressed with the formality of the audit trail..."* **[Open Bundle/Part B/§72C/pp143-144]**

d. What, if any, is the relevance of the fact that, until February 2015, it was neither confirmed nor denied that the Respondents carried out CNE activities at all?

108. In circumstances where the statutory regime has provided for property

interference by GCHQ in compliance with its statutory functions[36] since the introduction of the ISA 1994, it is not accepted that it is of any relevance that GCHQ did not admit to carrying out CNE activity until February 2015.

109. It is well understood by the Tribunal that national security considerations mean that much less is required to be put into the public domain (see *Liberty/Privacy* at §§38-39). Inevitably therefore there will be a tension between the development by eg. GCHQ of innovative technologies/techniques for property interference which national security considerations require to be kept secret and the extent to which such technologies/techniques can be addressed publicly. The fact that it was neither confirmed nor denied that GCHQ actually carried out such activities until February 2015 does not undermine the legality of the regime in circumstances where the statutory powers and functions of GCHQ could reasonably have been taken to include interference with computer equipment prior to that time.

e. What, if any, is the relevance of the Covert Surveillance and Property Interference Code, issued in 2002 and updated in 2010 and 2014?

110. As set out above, the Property Code is of particular relevance to the compatibility of the equipment interference regime with Article 8 ECHR prior to February 2015.

f. What, if any, is the effect of the publication of a Draft Equipment Interference Code of Practice in February 2015?

111. For reasons set out above, the draft Code provides more detailed provisions, but does not affect the Article 8 compliance of the regime given that the pre-February 2015 regime was also ECHR compliant.

g. What, if any, is the relevance of the Intelligence Services Commissioner's oversight of the use of the powers contained within ISA 1994?

112. The oversight provided by the Commissioner is a very important safeguard when assessing the overall ECHR compatibility of the regime for reasons already set out in detail above.

h. What, if any, is the relevance of the oversight by the Tribunal and the Intelligence and Security Committee of Parliament?

[36] GCHQ's statutory 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 ...."*.

113. The oversight provided by the ISC is also a very important safeguard when assessing the overall ECHR compatibility of the regime for reasons already set out in detail above.

LPP and Confidential Information

c. Have adequate safeguards been in place at all times to prevent the obtaining, storing, analysis or use of legally privileged material and other sensitive confidential documents?

114. In terms of the regime for the handling of legally privileged material, the Respondents accepted in the Belhaj IPT proceedings recorded in the Tribunal's Order dated 26 February 2015 namely that, "*since January 2010 the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material has contravened Article 8 ECHR and was accordingly unlawful*". Consistently with that, insofar as LPP material was obtained, analysed etc. it is accepted that the regime was unlawful in this earlier period.

115. The only issue that the Claimants have identified under this heading in these proceedings about the compatibility of the regime since February 2015 relates to the LPP provisions in respect of communications data. After being invited to clarify their case, the Claimants stated as follows[37]:

> "*The regime subsequent to the publication of the draft EI Code is not prescribed by law, because (in error of law) the draft Code does not recognise that communications data may be protected by LPP. These arguments will be familiar to the Tribunal and the Respondents. They were run by the Law Society in Belhaj (albeit it was not necessary for them to be ruled on in that case), and considered by the Divisional Court in R (Davis & Watson) v SSHD [2015] EWHC 2092 (Admin). Indeed, many of the same counsel were instructed in these cases*."

116. The Respondents do not accept that there is any error of law in the EI Code as contended for by the Claimants.

(a) The language which is used in the EI Code is not the same as that used in the Acquisition of Communications Data Code of Practice at §3.72ff[38]. In particular the EI Code refers in Chapter 3 to "*knowledge*

[37] see Bhatt Murphy's email of 12 November 2015 at 19:15.

[38] That Code states as follows:

> *3.72. Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.*

of matters subject to legal privilege" eg. in §3.6 **[Vol 1/CM1/p715]**. It does not contain any absolute statement that communications data is not subject to any form of professional privilege, in contrast to §3.72 of the Acquisition of Communications Data Code.

(b) In any event and without prejudice to that, the Divisional Court in *Davis and Watson* did not find the Acquisition of Communications Data Code to be unlawful in this regard, given the rare circumstances in which communications data might engage LPP and the protections which were in fact in place in the later provisions of that Code. Consequently at §§67-68 the Divisional Court stated:

> *"67. The Code of Practice issued by the Secretary of State states that communication data will not be subject to legal professional privilege since there will be no access to the contents of retained communications. The Law Society made written submissions which challenge the correctness of this statement. Reliance is placed on a dictum of Cotton LJ in Gardner v. Irvin (1878) 4 Ex D 49 at 83 where he said:-*
>
> > *"I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action".*
>
> *This approach was confirmed by Vinelott J in Derby v. Weldon (No 7) [1990] 1 WLR 1156.*
>
> *68.* ***No doubt such an example of privilege would rarely arise. However, communications with practising lawyers do need special***

3.73. However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament,94 or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

3.74. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

3.75. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see section 6 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner.

consideration. The same in our view can properly be said to apply to communications with MPs. The Code of Practice makes clear the need for such special attention." (emphasis added)

25 November 2015

JAMES EADIE QC
DANIEL BEARD QC
KATE GRANGE
RICHARD O'BRIEN