Neutral Citation Number: **[2016] UKIP Trib 14_85-CH**

IN THE INVESTIGATORY POWERS TRIBUNAL

P.O. Box 33220
London
SW1H 9ZQ
Date: 12/02/2016

Before :
MR JUSTICE BURTON (PRESIDENT)
MR JUSTICE MITTING (VICE-PRESIDENT)
MR ROBERT SEABROOK QC
MR CHARLES FLINT QC
THE HON CHRISTOPHER GARDNER QC
Between :

Case No. IPT 14/85/CH	**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	**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**

- -

Ben Jaffey and Tom Cleaver (instructed by **Bhatt Murphy Solicitors**) for the **Claimants**
James Eadie QC, Daniel Beard QC, Kate Grange and Richard O'Brien (instructed by **Government Legal Department**) for the **Respondents**
Jonathan Glasson QC, Counsel to the Tribunal (instructed by **Government Legal Department**)
Hearing dates: 1, 2 and 3 December 2015
Approved judgment

Mr Justice Burton (The President):

1. This is the judgment of the Tribunal.

2. This has been a hearing in respect of the claim by Privacy International, the well known NGO, and seven internet service providers, of which Greennet Limited carries on operations in this country and the other Claimants have customers in this country, though their main operations are based abroad. The hearing has been of preliminary issues of law, whose purpose is to establish whether, if the Second Respondent ("GCHQ") carries on the activity which is described as CNE (Computer Network Exploitation), which may have affected the Claimants, it has been lawful. The now well established procedure for this Tribunal is to make assumptions as to the significant facts in favour of claimants and reach conclusions on that basis, and only once it is concluded whether or not, if the assumed facts were established, the respondent's conduct would be unlawful, to consider the position thereafter in closed session. This procedure has enabled the Tribunal, on what is now a number of occasions, to hold open inter partes hearings, without possible damage to national security, while preserving, where appropriate, the Respondents' proper position of Neither Confirmed Nor Denied ("NCND").

3. Various possible different methods or consequences of CNE, or in its colloquial form 'hacking', as summarised in paragraph 9 below, have been canvassed in the witness statements produced on behalf of the Claimants by Mr Eric King, Professor Ross Anderson and Professor Peter Sommer, to which there have been responses, always subject to the constraints of NCND, in the witness statements of Mr Ciaran Martin, the Director General of Cyber Security at GCHQ. The particular significance of the use of CNE is that it addresses difficulties for the Intelligence Agencies caused by the ever increasing use of encryption by those whom the Agencies would wish to target for interception. The Claimants point out that CNE inevitably goes beyond interception, in accessing what is not and would not be communicated. The context of the issue is that the security situation for the United Kingdom, presently described as severe, is such that there needs to be the most diligent possible protection by the Respondents of the citizens and residents of the UK. Mr Martin points out in his first witness statement that even in the past year the threat to the UK from international terrorism in particular has continued to increase, and Mr Eadie QC for the Respondents submitted that proper protection of the citizen against terrorist attack is of the most fundamental importance, and that technological capabilities operated by the Intelligence Agencies lie at the very heart of the attempts of the State to safeguard the citizen against terrorist attack.

4. The sections of the Intelligence Services Act 1994 ("ISA") which have been primarily under consideration at this hearing are s.3, which sets out the powers of GCHQ, s.5 (with its machinery in part set out in s.6) and s.7. We shall refer to a s.5 warrant and a s.7 authorisation:

> "***3. The Government Communications Headquarters.***

(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be -

(a) 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; and

(b) to provide advice and assistance about—

(i) languages, including terminology used for technical matters, and

(ii) cryptography and other matters relating to the protection of information and other material,

to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

(2) The functions referred to in subsection (1)(a) above shall be exercisable only—

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime.

…

5 Warrants: general.

(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is

authorised by a warrant issued by the Secretary of State under this section.

(2) The Secretary of State may, on an application made by . . . GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State -

(a) thinks it necessary for the action to be taken for the purpose of assisting . . .

(iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and

(b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;

(c) is satisfied that satisfactory arrangements are in force under section 2(2)(a) of the [Security Service Act 1989 ("the 1989 Act")] *(duties of the Director-General of the Security Service), section 2(2)(a) above or section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements.*

(2A) The matters to be taken into account in considering whether the requirements of subsection (2)(a) and (b) are satisfied in the case of any warrant shall include whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means.

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

(3A) A warrant issued on the application of the Security Service for the purposes of the exercise of their function under section 1(4) of the Security

Service Act 1989 may not relate to property in the British Islands unless it authorises the taking of action in relation to conduct within subsection (3B) below.

(3B) Conduct is within this subsection if it constitutes (or, if it took place in the United Kingdom, would constitute) one or more offences, and either -

(*a*) *it involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose; or*

(b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.

(4) Subject to subsection (5) below, the Security Service may make an application under subsection (2) above for a warrant to be issued authorising that Service (or a person acting on its behalf) to take such action as is specified in the warrant on behalf of the Intelligence Service or GCHQ and, where such a warrant is issued, the functions of the Security Service shall include the carrying out of the action so specified, whether or not it would otherwise be within its functions.

(5) The Security Service may not make an application for a warrant by virtue of subsection (4) above except where the action proposed to be authorised by the warrant—

(a) is action in respect of which the Intelligence Service or, as the case may be, GCHQ could make such an application; and

(b) is to be taken otherwise than in support of the prevention or detection of serious crime

6 Warrants: procedure and duration, etc.

(1) A warrant shall not be issued except—

(a) under the hand of the Secretary of State or in the case of a warrant by the Scottish Minister (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive; or

(b) in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; or

(c) in an urgent case where, the Scottish Ministers have (by virtue of provision made under section 63 of the Scotland Act 1998) expressly authorised its issue and a statement of that fact is endorsed thereon, under the hand of a member of the staff of the Scottish Administration who is in the Senior Civil Service and is designated by the Scottish Ministers as a person under whose hand a warrant may be issued in such a case.

(d) *in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of the specified officials.*

(1A) But a warrant issued in accordance with subsection (1) (d) may authorise the taking of an action only if the action is an action in relation to property which, immediately before the issue of the warrant, would, if done outside the British Islands, have been authorised by virtue of an authorisation under section 7 that was in force at that time.

(1B) A senior official who issues a warrant in accordance with subsection (1)(d) must inform the Secretary of State about the issue of the warrant as soon as practicable after issuing it."

(2) A warrant shall, unless renewed under subsection (3) below, cease to have effect—

(a) if the warrant was under the hand of the Secretary of State or, in the case of a

warrant issued by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive, at the end of the period of six months beginning with the day on which it was issued; and

(*b*) *in any other case, at the end of the period ending with the second working day following that day.*

(3) If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of six months beginning with that day.

(4) The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary.

(5) In the preceding provisions of this section "warrant" means a warrant under section 5 above.

. . .

7 Authorisation of acts outside the British Islands.

(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

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

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

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

function of the Intelligence Service or GCHQ; and

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

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

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

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

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

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

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

(c) may be subject to conditions so specified.

(5) An authorisation shall not be given under this section except -

(a) under the hand of the Secretary of State; or

(b) in an urgent case where the Secretary of State has expressly authorised it to be

given and a statement of that fact is endorsed on it, under the hand of a senior official.

(6) An authorisation shall, unless renewed under subsection (7) below, cease to have effect -

(a) if the authorisation was given under the hand of the Secretary of State, at the end of the period of six months beginning with the day on which it was given;

(b) in any other case, at the end of the period ending with the second working day following the day on which it was given.

(7) If at any time before the day on which an authorisation would cease to have effect the Secretary of State considers it necessary for the authorisation to continue to have effect for the purpose for which it was given, he may by an instrument under his hand renew it for a period of six months beginning with that day.

(8) The Secretary of State shall cancel an authorisation if he is satisfied that any act authorised by it is no longer necessary.

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

(a) is done in the British Islands; but

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

and in this subsection "apparatus " has the same meaning as in [RIPA].

(10) Where–

(a) a person is authorised by virtue of this section to do an act outside the British Islands in relation to property,

(b) the act is one which, in relation to property within the British Islands, is

capable of being authorised by a warrant under section 5,

(c) a person authorised by virtue of this section to do that act outside the British Islands, does the act in relation to that property while it is within the British Islands, and

(d) the act is done in circumstances falling within subsection (11) or (12),

This section shall have effect as if the act were done outside the British Islands in relation to that property.

(11) An act is done in circumstances falling within this subsection if it is done in relation to the property at a time when it is believed to be outside the British Islands.

(12) An act is done in circumstances falling within this subsection if it–

(a) is done in relation to property which was mistakenly believed to be outside the British Islands either when the authorisation under this section was given or at a subsequent time or which has been brought within the British Islands since the giving of the authorisation; but

(b) is done before the end of the fifth working day after the day on which the presence of the property in the British Islands first becomes known.

(13) In subsection (12) the reference to the day on which the presence of the property in the British Islands first becomes known is a reference to the day on which it first appears to a member of the Intelligence Service or of GCHQ, after the relevant time–

(a) that the belief that the property was outside the British Islands was mistaken; or

(b) that the property is within those Islands.

(14) In subsection (13) 'the relevant time' means, as the case may be –

(a) the time of the mistaken belief mentioned in subsection (12)(a); or

(b) the time at which the property was, or was most recently, brought within the British Islands."

5. The 'assumed facts' procedure has been impacted to an extent on this occasion by virtue of the fact that there has been a considerable degree of acceptance by the Respondents, or 'avowal' as it has been called, of the existence and use of CNE by GCHQ, and certainly so since the publication on 6 February 2015, during the course of, and seemingly as a direct result of, the existence of these proceedings, of the draft Equipment Interference Code of Practice pursuant to s.71 of the Regulation of Investigatory Powers Act 2000 ("RIPA") ("the E I Code"), which has now, after a period of consultation, been laid before Parliament in November 2015. [Since the hearing, it has been brought into force by S.I.2016 no.38 dated 14 January 2016]. As a result of a Schedule of Avowals, helpfully prepared by Mr Jaffey of counsel on behalf of the Claimants, and responded to by the Respondents, the following matters are admitted:

i) GCHQ carries out CNE within and outside the UK.

ii) In 2013 about 20% of GCHQ's intelligence reports contained information derived from CNE.

iii) GCHQ undertakes both "*persistent*" and "*non-persistent*" CNE operations, namely both where an 'implant' expires at the end of a user's internet session and where it "resides" on a computer for an extended period.

iv) CNE operations undertaken by GCHQ can be against a specific device or a computer network.

v) GCHQ has obtained warrants under s.5 and authorisations under s.7, and in relation to the latter had five s.7 class based authorisations in 2014.

6. Apart from the provisions of the ISA, the other most material statutory provisions are as follows:

i) The 1989 Act (referred to above) by s.3 gave the power to the Security Service ("MI5") to apply for a warrant, which it is common ground could have authorised conduct by GCHQ (whose existence was not at that stage publicly admitted) on its behalf, whereby the Secretary of State could, on an application made by MI5 issue a warrant "*authorising the taking of such action as is specified in the warrant in*

respect of any property so specified" in the circumstances there provided for. This provision was replaced by ISA in 1994.

ii) The Official Secrets Act 1989 makes it an offence for a member of the Security and Intelligence Services by s.1 to disclose information relating to security or intelligence without lawful authority and by s.8 to retain it without lawful authority or fail to take proper care to prevent unauthorised disclosure of it.

iii) A similar provision to safeguard information obtained by any of the Intelligence Services, by limiting its disclosure and use to the proper discharge of any of their functions (including the interests of national security) is in s.19 of the Counter-Terrorism Act 2008.

iv) The provisions of the Data Protection Act 1998 preserve (notwithstanding any exemptions) the obligation on GCHQ to comply with the Fifth and Seventh data protection principles, namely:

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

7. The Respondents accept and assert that as a matter of public law they have been bound since February 2015 by the draft E I Code, which was accompanied by a Ministerial statement to that effect. We are satisfied that that is the case. Prior to such publication, there was the Covert Surveillance and Property Interference Code (the "Property Code"), also pursuant to s.71 of RIPA, which has been materially in its present form since 2002. The Property Code continues in force, but under paragraph 1.2 of the E I Code where there is an overlap between the two Codes the E I Code takes precedence.

8. The parties agreed a List of Issues to be resolved at the hearing, which were agreed during the period of preparation for the hearing as a result of excellent cooperation between the parties, and with the very considerable assistance of Jonathan Glasson QC, Counsel for the Tribunal. As a result of the very careful preparation for, and the concise and persuasive presentation at, the hearing by both parties, it was possible to conclude the oral argument in 3 days. There was a degree of context for the resolution of the issues, not just by reference to the witness statements to which we have referred. The Respondents accept that the provisions of Articles 8 and 10 of the European Convention of Human Rights, which we do not need to set out, apply to Privacy International as a campaigning NGO, and, at least for the purposes of this hearing, that they both apply to the internet companies: in any event there is no material difference in the applicability of both Articles, which have been, as in previous hearings, argued in tandem. As to other matters:

i) Both parties accepted at this hearing the effect of this Tribunal's conclusions in what have become known as **Liberty/Privacy (No.1)** [2015] 3 AER 142 and **(No.2)** [2015] 3 AER 212. It was common ground that all the material decisions of the ECtHR were fully canvassed in **Liberty/Privacy (No.1)** and their effect set out in that Judgment. The consequence was that there was a great deal less need to refer to the underlying ECtHR Judgments themselves in the hearing before us, and it was common ground that the only material ECtHR decision since **Liberty/Privacy** is **R.E. v United Kingdom** (Application No.62498/11), Judgment 27 October 2015, to which we were referred by both sides.

ii) As in **Liberty/Privacy**, emphasis was placed by the Respondents on the existence of oversight of the security arrangements and procedures by the Intelligence and Security Committee of Parliament ("ISC") and by the Commissioners. In this case the relevant Commissioner is the Intelligence Services Commissioner, Sir Mark Waller, on whose Reports both sides relied. As is to be expected, and will be referred to below, Sir Mark's responsibility included drawing attention to areas which, upon his inspection of the Intelligence Services, he felt could be improved; but there is no doubt, by reference to those Reports, that it continues to be his view, as expressed in his 2013 Report, that "*GCHQ's staff continue to conduct themselves with the highest level of integrity and legal compliance*". The ISC's latest report of 12 March 2015 is to similar effect.

9. It was agreed for the purpose of the List of Issues (at paragraph 6) that CNE might be used by GCHQ so as to involve the following:

a) The obtaining of information from a particular device, server or network.

That constituted part of the Respondents' avowals, and consequently was no longer subject to NCND. As to the balance of the original paragraph 6 of the List of Issues:

b) The creation, modification or deletion of information on a device, server or network.

It was accepted at paragraph 46 of Mr Martin's First Statement that CNE could theoretically change the material on a computer, e.g. by way of an implant. In the light of that, coupled with the acceptance generally by GCHQ that it carries out CNE activities, GCHQ accepts that it has avowed the creation (to the extent that the placing of an implant on a device amounts to the creation of information) and modification of information on a device and this is no longer subject to NCND. In addition, whilst GCHQ accepts that creating or modifying information on a server or network could lawfully occur, this is neither confirmed nor denied.

But apart from that, sub-paragraph (b) is neither confirmed nor denied.

c) The carrying out of intrusive surveillance.

This is neither confirmed nor denied, although GCHQ has accepted that the use of CNE techniques may be intrusive.

d) The use of CNE in such a way that it creates a potential security vulnerability in software or hardware, on a server or on a network.

This is not avowed. However it has been accepted that any CNE operations which are carried out by GCHQ are conducted in such a way as to minimise the risk of leaving target devices open to exploitation by others (see paragraph 39 of Mr Martin's First Statement).

e) The use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest.

This has been characterised as 'bulk CNE'. The Respondents agree that this could arise pursuant to the powers of GCHQ within the scope of a s.7 authorisation, but neither admit nor deny that it has ever occurred, and Mr Martin in his third witness statement says that it is "s*imply not correct to assert that GCHQ is using CNE on an indiscriminate and disproportionate scale*".

f) The use of CNE to weaken software or hardware at its source, prior to its deployment to users.

This is neither confirmed nor denied.

g) The obtaining of information for the purpose of maintaining or further developing the intelligence services' CNE capabilities.

This is neither confirmed nor denied.

10. The List of Issues, shorn of its paragraph 6 in which the above matters (a) to (g) were canvassed, appears as Appendix I to this Judgment. We turn to address those issues below, although not quite in the same format.

11. The value of these proceedings in open court before us has been to our mind again emphasised, whatever the outcome, by virtue of the full inter partes consideration of such issues, and in particular:

i) The knock-on effect that the very existence of these proceedings has clearly had. We have already noted the fact that the publication of the draft E I Code was on 6 February 2015, revealing for the first time in public the use by GCHQ of CNE and the procedures under which it is

to operate (in particular at paragraph 1.9 "*Equipment Interference is conducted in accordance with the statutory functions of each Intelligence Service*"). That was the same date as the service of the Respondents' Open Response in these proceedings, setting out their case as to CNE. The Claimants have pointed to the fact that within a month after the initiation in May 2014 of these proceedings by Privacy International, by which the Claimants raised the issue as to the import of s.10 of the Computer Misuse Act 1990 ("CMA"), proposed amendments to s.10 were laid before Parliament on 5 June 2014 (as part of the Serious Crime Bill), which have now been enacted. These amendments are said by the Respondents to clarify, but asserted by the Claimants to change, the nature of the un-amended s.10, which forms the basis of the discussion in Issue 1 below, and plainly were also a consequence of these proceedings.

ii) There are now in the public domain what were previously "*below the waterline*" arrangements (see paragraph 7 in the **Liberty/Privacy No.1** judgment) underlying both the Property Code and the E I Code, either redacted or gisted. Whether or not in the event they are determinative in relation to the issues canvassed before us in relation to the question of accessibility or foreseeability under Articles 8 and 10 of the ECHR, it is valuable that they have been produced by the Respondents in these proceedings. This arose as a result of the disclosure sought by the Claimants, and by Counsel to the Tribunal, and requested by the Tribunal.

iii) Simultaneously with the preparation and eventual presentation of this case, there has been the consideration by David Anderson QC, the Independent Reviewer of terrorism legislation, in his Report dated June 2015, and subsequently the draft Investigatory Powers Bill ("the IP Bill") laid before Parliament in November 2015, which in its present form has been before us, both of which plainly drew upon the ideas and submissions which have now been openly canvassed before us.

Issue 1: s.10 CMA

12. The first Issue is: Was an act which would be an offence under s.3 of the CMA made lawful by a s.5 warrant or s.7 authorisation, prior to the amendment of s.10 CMA as of May 2015?

13. The following is common ground:

i) S.1 of CMA reads in material part as follows:

"***1. Unauthorised access to computer material.***

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any

computer, or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

. . .”

ii) S.3 reads as follows:

“***3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.***

(1) A person is guilty of an offence if -

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act -

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section -

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

. . . "

iii) An act of CNE, insofar as it consists of, for example, removing or replacing information on a computer, would not simply constitute an offence under s.1 but plainly also under s.3 (unless exempt from sanction).

iv) Since 3 May 2015 the amendment to s.10 (referred to in paragraph 11(i) above) makes it clear that a person acting under a s.5 warrant or s.7 authorisation commits an offence neither under s.1 nor under s.3 of the CMA.

So the only issue relates to the period prior to 3 May 2015.

14. S.10 of the CMA prior to its amendment read as follows:

"*10. Saving for certain law enforcement powers*

Section 1(1) above has effect without prejudice to the operation –

(a) In England and Wales of any enactment relating to powers of inspection, search or seizure; and

(b) In Scotland of any enactment or rule of law relating to powers of examination, search or seizure.

. . ."

15. S.10 as amended by the Serious Crime Act 2015 s.44(2)(a) now reads as follows:

"10. Savings

Sections 1 to 3A have effect without prejudice to the operation -

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure or of any other enactment or rule of law by virtue of which the conduct in question is authorised or required.

and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of any of those sections. In this section—

"enactment" means any enactment, whenever passed or made, contained in—

(a) an Act of Parliament;
(b) an Act of the Scottish Parliament;
(c) a Measure or Act of the National Assembly for Wales;
(d) an instrument made under any such Act or Measure;
(e) any other subordinate legislation (within the meaning of the Interpretation Act 1978)

. . .".

16. The Claimants submit that until the passage of this amendment to s.10 any act of CNE which would contravene s.3 of the CMA was unlawful. On the Claimants' case, the effect of the amendment is to reverse the previous position; hence the need for it. The Respondents submit however that the amendment to s.10 was simply clarificatory. This the Respondents submit was made clear by the Home Office Circular (Serious Crime Act 2015) and the Home Office Fact sheet, both dated March 2015, which accompanied the bill. It is not contested that such documents are admissible in construction of

the bill which they accompanied, but it is equally accepted that those documents cannot provide any aid to construction of the original 1990 CMA.

17. Mr Jaffey submits that:

i) The CMA is the '*lex specialis*' relating to computer misuse. It governs the position, and there is specific reference in the unamended s.10 to the law enforcement powers which are exempted from the ambit of s.1, and s.3 is left entirely unaffected. When the ISA was enacted in 1994, it could not affect the position, namely that it is only s.1 of the CMA which has effect "*without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure*", and not s.3

ii) There may be good reason for Parliament having so differentiated because:

(a) Parliament is to be taken to have decided that less intrusive operations would be exempted from the ambit of the Act and not the more excessive activity covered by s.3.

(b) It may be that there were concerns that an act which would contravene s.3 might impact upon the reliability of evidence contained in a computer, in the context of its being admitted into evidence in subsequent criminal proceedings (there being no bar on the admission of such evidence, as there is and was in relation to intercept evidence). There is some discussion in **Hansard** at the time of passage of the bill as to concerns about the position of such evidence.

iii) The 1990 CMA, and its express savings, cannot be impliedly overruled by the subsequent 1994 ISA (see Lord Hope in **H v Lord Advocate** [2013] 1 AC 413 at 436, paragraph 30 as to implied subsequent repeal).

18. Mr Eadie submits that:

i) The language of ss.5 and 7 of the ISA, set out in paragraph 4 above is in each case clear. No act done pursuant to those sections can be unlawful either civilly or criminally. That plainly includes an act which would otherwise be an offence under s.3 of the CMA.

ii) The 1994 ISA was the '*lex specialis*' relating to the Intelligence Agencies. Earlier savings provisions cannot limit the powers given under s.5 and s.7 of ISA. S.10 of CMA (as un-amended) did not purport to be exhaustive: the heading, which is admissible for interpretation, refers to "*saving for certain law enforcement powers*", and even the words "*any enactment relating to powers of inspection, search or seizure*" would only appear to be relevant in relation to s.1 of CMA and not necessarily to s.3. In any event s.5 and s.7 post-date the CMA, and expressly authorise and exempt from sanction the relevant conduct, and it would be unthinkable that acts under it, in accordance

with GCHQ's express powers under s.3(1)(a), would be unlawful. Ss.5 and 7 are not, and are not relied upon as, an implied repeal of what was only a savings clause in the 1990 Act.

iii) With regard to the 1990 discussion in **Hansard**, there is no sign that concerns about the admissibility of evidence were discussed in the specific context either of s.3 or of (what became) s.10. In any event it is plain from **Hansard** that there was an amendment put forward, which would have placed what was called a temporary stop (pending further debate) preventing the Security Service from misusing computers (this would have been pursuant to s.3 of the 1989 Act referred to in paragraph 6(i) above). This amendment ("*to prevent hacking or similar activities by the Security Service*") was not pressed. It would seem therefore that it was accepted that the 1989 Act, already on the statute book, was not affected by the CMA. *A fortiori* the subsequent 1994 Act is not either.

19. We would add that if reference is made to the definition section in s.17 of the CMA there is not in fact a dramatic difference between *securing access* under s1 and acts covered by s.3 in any event. S.17(2) reads as follows:

> "*(2) A person secures access* [our underlining] *to any program or data held in a computer if by causing a computer to perform any function he –*
>
> *(a) Alters or erases the program or data;*
>
> *(b) Copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*
>
> *(c) Uses it; or*
>
> *(d) Has it output from the computer in which it is held (whether by having it displayed or in any other manner).*
>
> *And references to access to a program or data (and to an intent to secure such access . . .) shall be read accordingly.*"

Any concern about potential impact on computers for subsequent admissibility purposes would be as live in respect of such a wide definition of s.1 as it would be in respect of s.3.

20. Whatever was the purpose lying behind the precise wording of s.10 in its un-amended form, it seems to us clear that it had no effect upon and/or was expressly overtaken by the clear words of ss.5 and 7 of the ISA. It would indeed be extraordinary that proportionate and necessary steps taken for the

(permitted) purpose of protecting national security, taken under an express power under ss.5 or 7 of the ISA, and covered by an express removal of civil or criminal liability, could be rendered unlawful by reference to a saving under an earlier statute. The inability lawfully to take such steps under ss.5 and 7 would render the very function of GCHQ in relation to computers provided for in s.3 of ISA (set out in paragraph 4 above), including powers to "*monitor or interfere with electro magnetic, acoustic and other emissions . . . in the interests of national security*", entirely nugatory. Any argument in support of such an extraordinary outcome has been removed by the amendment, which is, we are satisfied, simply clarificatory, and we accept Mr Eadie's submissions.

Issue 2: Territorial jurisdiction in respect of ss.5/7

21. The Issue was: If an act by the Respondents constituting CNE was unlawful prior to May 2015, would any such act abroad have been unlawful?

22. S.4 of the CMA provides that it is immaterial whether any act occurred in the UK or whether the accused was in the UK at the time of any such act, provided that there was *"at least one significant link with domestic jurisdiction"* at the relevant time. By s.5, where the accused was in a country outside the UK at the time of the act constituting the offence, there would be such a significant link with domestic jurisdiction if the accused was a UK national at the time, and the act in question constituted an offence under the law of the country in which it occurred.

23. As we have decided Issue 1 in favour of the Respondents, this issue 2 does not arise. Suffice it however to say that the jurisdictional provisions of ss.4 and 5 of the CMA are very broad, and s.4 (2) provides that: "*at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed*". The question could therefore only arise if there is no such significant link. Mr Jaffey sought to contend that s.31 of the Criminal Justice Act 1948 would render a Crown servant, such as an employee of GCHQ, criminally liable in such a case because it provides that "*any British subject employed under His Majesty's Government in the United Kingdom in the service 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*". Although in the event we do not have to answer this issue, it appears clear to us that, in order for s.31 to avail, there would need to have been an offence under the CMA, which there would not have been if there was no *significant jurisdictional link*, and in any event, just as with the CMA itself, there would be the requirement to prove 'double criminality'. As it is, Issue 2 does not specifically require to be answered, but we conclude that any act abroad pursuant to ss.5 or 7 of the ISA which would otherwise be an offence under ss.1 and/or 3 of the CMA would not be unlawful.

Issue 3: Intangible property

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

25. There is no definition of *property* in s.5 of the ISA. The relevant provision, set out above, simply refers to a warrant "*authorising the taking . . . of such action as is specified in the warrant in respect of* <u>*any property*</u> [our underlining] *so specified or in respect of wireless telegraphy so specified*". On the face of it, not only is the definition of property not limited to real or personal property, but there is nothing to exclude intangible property. The definition "*any property*", would appear to include it, and this is emphasised by the inclusion as an alternative subject matter of the warrant of "*wireless telegraphy*".

26. There appear to be two matters which led the Claimants to pursue this argument:

    i) The reference in a document published by Mr Snowden, and exhibited by the Claimants, to there possibly being a s.5 warrant which permitted interference with computer software in breach of copyright and licensing agreements.

    ii) The reference in s.5(3), and in s.5(3A) (for MI5), to the inapplicability of certain warrants in respect of "*property in the British Islands*". Mr Jaffey said that this is an inapt reference if intangible property is intended. But there appears to us to be no answer either to Mr Beard QC's succinct submissions on this topic for the Respondents, including the point that as defined by statute copyright is a collection of rights in respect of the United Kingdom, or to that put by the Tribunal in relation to choses in action such as bank accounts, which again would have a geographical identity.

27. The whole of this contention seemed to us to evaporate in the course of argument, when Mr Jaffey accepted (Day 1/127, 138, Day 2/14-16) that physical interference with property in the context of CNE authorised by a s.5 warrant may also involve an interference with copyright, which would then be taken to be authorised, as compared with what he called a "*pure interference with intellectual property rights*", i.e. that interference with copyright would be authorised if ancillary to interference with physical property.

28. We can see no justification whatever for such a construction of the Statute. We are satisfied that s.5 extends to intangible property, whether the action is directed at intangible property alone or is ancillary to interference with physical property. We note that this is also the view of the Intelligence Services Commissioner (page 17 of his Report of 25 June 2015). A s.5 warrant is as sufficient authority for such interference as is s.50 of the Copyright Designs and Patents Act 1988, whereby "*where the doing of a particular act is specifically authorised by an Act of Parliament, whenever passed, . . . the doing of that act does not infringe copyright*".

29. An argument in relation to the possible impact of the EU Copyright Directive (2001/29/EC), raised by Mr Jaffey in his pleadings and his skeleton argument, was not pursued.

30. Accordingly we resolve this issue in favour of the Respondents.

Issue 4: "Thematic warrants" and the requirement for specification under s.5

31. We have set down the words "*thematic warrants*" in the above heading, because the words are used in the Agreed Issues. However, not only do such words have no statutory basis, but such description does not appear to us to capture the reality of the issue which we have to decide. The words first appear in a completely different context, namely at page 21 of the ISC Report of 12 March 2015, a passage in which interception warrants under s.8(1) of RIPA were being discussed.

32. S.8(1) provides that:

> "*(1) An interception warrant must name or describe either -*
>
> *(a) one person as the interception subject; or*
>
> *(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.*"

The ISC state in their Report in a section under the heading "*Thematic warrants*" as follows:

> "*42. While the very significant majority of 8(1) warrants relate to one individual, in some limited circumstances an 8(1) warrant may be thematic. The term 'thematic warrant' is not one defined in statute. However, the Home Secretary clarified that Section 81 of RIPA defines a person as "[including] any organisation* [and] *any association or combination of persons", thereby providing a statutory basis for thematic warrants. The Home Secretary explained that "the group of individuals must be sufficiently defined to ensure that I, or another Secretary of State, is reasonably able to foresee the extent of the interference and decide that it is necessary and proportionate"*
>
> *43. MI5 have explained that they will apply for a thematic warrant "where we need to use the same capability on multiple occasions against a defined group or network on the basis of a consistent necessity and proportionality case . . . rather than [applying for] individual warrants against each member of the group.*"

There is then discussion by reference to the issue of a s.8(1) warrant in the context of a number of circumstances where it may be appropriate to grant such a warrant by reference to a group linked by a specific intelligence requirement. The thematic reference is obviously because of the wide coverage of an (otherwise specific) s.8(1) warrant by virtue of the broad definition of '*person*' in s.8(1).

33. The description is taken up by the Intelligence Services Commissioner at paragraph 849 of his 2014 Report at page 18, which reads (though now in the context of a s.5 warrant) 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 <u>submission</u> and the <u>warrant</u> must be set out in a way which allows the*

Secretary of State to make the decision on necessity and proportionality."

It is plainly from this passage that Mr Jaffey has drawn the basis for his submissions set out below, and which have led to the formulation of Issue 4.

34. We prefer however to phrase Issue 4 as: What is the meaning of the words *'in respect of any property so specified'* for the purposes of the issue of a s.5 warrant?

35. Mr Jaffey submits as follows:

i) The common law sets its face against general warrants, as is well known from the seminal Eighteenth Century cases such as **Entick v Carrington** [1765] 2 Wilson KB 275 and **Money v Leach** [1765] 3 Burr 1742. As for statute law, he relies on Lord Hoffmann in **R v Secretary of State for the Home Department, Ex p Simms** [2000] 2 AC 115 at 131: "*Fundamental rights cannot be overridden by general or ambiguous words*". Thus he takes as a starting point that such words as were disapproved in the warrant in **Money v Leach**, relating to searching for and seizing the papers of the authors, printers and publishers of the North Briton (wheresoever found), should not be permitted pursuant to a s.5 warrant, or that a s.5 warrant should not be defined so as to permit "*any property so specified*" to include such a provision.

ii) He contrasts the provision in s.5(2) for a warrant "*in respect of any property so specified*" with the authorisation provided for in s.7, only available in respect of *acts outside the British Islands*, which by s.7(4) "*may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified*". This latter is, and was described by the Intelligence Services Commissioner in the passage from his Report quoted above as, a '*class authorisation*'. It relates effectively to any operation carried out abroad by the Agencies: and there is provision within the E I Code (paragraphs 7.11-7.14) for situations where, because "*an authorisation under section 7 may relate to a broad class of operations*" (7.11), "*Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference should be sought from a designated senior official*"(7.12). Mr Jaffey submits that this emphasises the difference between a s.7 authorisation and a s.5 warrant. The former can authorise a broader class of operation, but is subject to specific subsequent approvals, whereas the latter is not subject to any such protective or limiting provision.

iii) Mr Jaffey accepts that the property specified in a s.5 warrant may include a reference to more than one person or more than one place, up to an unlimited number, provided they are properly specified. But he submits that it must not extend to authorising an entire operation or

suite of operations, and that identification cannot depend upon the belief, suspicion or judgment of the officer acting under the warrant. It must also be possible to identify the property/equipment at the date of the warrant. Thus a warrant permitting CNE in respect of computers owned or used by any diplomatic representatives of the State of Ruritania, or by any member of a named proscribed organisation, is not adequate because (i) who they are is thus left open (unless a list of names is provided to be attached to the warrant); (ii) it is not limited to those who are part of that group at the time of the warrant; (iii) it leaves too much to the belief, suspicion or judgment of the officer, and deprives a Secretary of State of the opportunity to exercise his required discretion as to the necessity and proportionality of the warrant. Mr Jaffey submitted (Day 2/12) that the Secretary of State had to consider before granting a warrant whether or not such intrusion would be justified in the case of each individual.

iv) Mr Jaffey had made reference to **Hansard** in respect of discussion in Parliament in 1989, prior to the passage of the Security Service Act 1989, but both parties agreed that this was of no assistance. However Mr Jaffey also referred to the IP Bill, referred to in paragraph 11(iii) above, for the purpose of showing what is now proposed, by reference to clause 83 in Part 5 of the Bill. The IP Bill provides, by clause 81, for a new warrant, to be called a "*targeted equipment interference warrant*", and the broad definition of the subject matter of such proposed warrant is set out in clause 83, including eight permitted such targets including, by way of example "*(a) equipment belonging to, used by or in the possession of the particular person or organisation*" and "*(b) equipment belonging to, used by or in the possession of persons who form a group that shares a common purpose or who carry on, or maybe carrying on, a particular activity*". His submission is that such defined targets are much wider than what he submits is the more limiting ambit of a s.5 warrant.

36. Mr Eadie responds as follows:

i) As to the Eighteenth Century common law cases, they are at best of marginal relevance. They plainly relate to the limitation on common law powers in relation to executive acts within the United Kingdom. S.5 is not limited to acts within the United Kingdom and in any event is a creature of statute. The legislative context and intent relate to the powers of the Secretary of State in respect of the protection of national security, and substantial limitation is imposed by the requirement of the section itself to consider whether the warrant falls within the statutory purposes of the agency applying for it (s.3(1) so far as concerns GCHQ) ("legality"), necessity and proportionality. The word "*specified*" is used three times in s.5(2), relating to the actions sought to be authorised and in respect of any property or "*wireless telegraphy*". He submits that what is required is the best description possible. Even a s.8(1) warrant under RIPA, which is expressly more limited, can have a broad ambit, as discussed in paragraph 32 above,

and the inclusion of "*wireless telegraphy*" in the section is significant, being very broadly defined (see s.11(e) of the ISA) by reference to what was then the Wireless Telegraphy Act 1949 (now 2006), and, as Mr Jaffey accepted, could extend to an entire communications frequency or a group of communications frequencies.

ii) S.7 is a different provision. It relates to the "*Authorisation of acts outside the British Islands*", and is not in direct contrast with, or alternative to, s.5 (in the way for example that s.8(1) and s.8(4) fall to be contrasted in RIPA). Mr Jaffey accepts that a s.5 warrant can extend to property owned or used by a group of persons, and there may therefore be occasions in which the scope of a s.5 warrant may cover similar conduct to an operation which, if overseas, could be sanctioned under s.7, but it is nevertheless directed at specified property. Only in 2001 was s.7 amended so as to add the power for GCHQ to seek a s.7 authorisation, by the Anti-terrorism, Crime and Security Act 2001. Until then GCHQ could only rely on s.5. Thus in any event there was no such contrast between s.5 and s.7 so far as concerned GCHQ at the date of the passage of the Act.

iii) Mr Eadie does not accept any of the limiting propositions set out in paragraph 35(iii) above. He submits that the requirement is for the actions and property to be objectively ascertainable. The examples referred to above, both as to Ruritania and proscribed organisations, are in his submission entirely proper and adequate. It is not necessary to identify persons any more than is possible at the time of the issue of the warrant, and it is certainly not necessary for the individuals to be identified by name or by reference to the particular time when the warrant is issued. A warrant could cover, in the examples given, anyone who was at any time during the duration of the warrant (six months unless specifically renewed) within the defined group. What is important is that an application for a warrant contains as much information as possible to enable a Secretary of State to make a decision as to whether to issue a warrant, and, if so, as to its scope. This might involve reducing or putting a limit on the persons or category of persons covered, or defining property by reference to such a restriction. He submits that what is fundamental is the duty imposed on the Secretary of State to consider whether the warrant is within the powers of the agency applying for it (legality) and whether the issue of the warrant would satisfy the tests of necessity and proportionality. That is the discipline referred to in paragraph 88 of **R (Miranda) -v- Secretary of State for The Home Department** [2014] 1 WLR per Laws LJ. [1] Mr Jaffey points out that the requirement for proportionality was not introduced into s.5 by amendment until after the introduction of the Human Rights Act 2000, by the passage of RIPA, and that it cannot have been intended thereby to alter the scope of a lawful warrant under s.5. Mr Eadie points to the words of Lord Toulson in **R**

[1] The decision in the Court of Appeal ([2016] EWCA Civ.6), subsequent to the hearing before us, does not question the importance of this discipline, but considers the overlay of Article 10 in relation to press freedom (per Lord Dyson MR at paras 98-117).

(Brown) v Secretary of State for the Home Department [2015] UKSC 8 at paragraph 24, as to the relevance of a subsequent amendment to interpretation of the statute. In any event he is content to rely if necessary on the duties of the Secretary of State as to legality and necessity already, as he puts it, "*hard-wired*" into s.5 prior to 2000. He submits that the words of the North Briton warrant, referred to in paragraph 35(i) above, would, subject to questions of necessity and proportionality in the particular circumstances, certainly be sufficiently specified. Another example canvassed in the course of the hearing was "*all mobile phones in Birmingham*". This could, submitted Mr Eadie, be sufficiently *specified*, but, save in an exceptional national emergency, would be unlikely to be either consistent with necessity or proportionality or with GCHQ's statutory obligations.

iv) Mr Eadie submits that (as is indeed said in its accompanying Guide) the IP Bill, albeit in respect of a differently named warrant, brings together powers already available, and the descriptions of targets in the new proposed clause 83 would, subject to the requirements of necessity and proportionality, all be consistent with the existing s.5.

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

38. The issue as to whether the specification is sufficient in any particular case will be dependent on the particular facts of that case. The courts frequently have to determine such questions for example in respect of a warrant under the Police Act 1997 s.93, when the issues, by reference to the particular facts would be fully aired in open. That is not possible in relation to a s.5 warrant, but it may still be subject to scrutiny by the Intelligence Services Commissioner, by the ISC and, if and when a complaint is made to this Tribunal, then by this Tribunal. But the test is not in our judgment different - Are the actions and the property sufficiently identified? The Home Secretary's own words as recorded in paragraph 42 of the ISC Report, set out in paragraph 32 above, relating to a s.8(1) warrant, are applicable here also. It is not in our judgment necessary for a Secretary of State to exercise judgment in relation to a warrant for it to be limited to a named or identified individual or list of individuals. The property should be so defined, whether by reference to persons or a group or category of persons, that the extent of the *reasonably foreseeable interference* caused by the authorisation of CNE in relation to the actions and property specified in the warrant can be addressed.

39. As discussed in the course of argument, the word under consideration is simply *specified*, and this may be contrasted with other statutes such as those relating to letters of request, where the requirement of the Evidence (Proceedings in Other Jurisdictions) Act 1975 is for "*particular documents specified*". There is no requirement here for specification of *particular*

property, but simply for specification of the property, which in our judgment is a word not of limitation but of description, and the issue becomes one simply of sufficiency of identification.

40. The statute does not fall to be interpreted by reference to the underlying Code, in particular one which, like the E I Code, has been in draft waiting to be approved by Parliament. But what is of course important is what is put in the applications to the Secretary of State, so that he can exercise his discretion lawfully and reasonably. Both in the Property Code, in place since 2002, (at paragraphs 7.18-7.19) and now in the E I Code (at paragraph 4.6), there is a lengthy list of what is required to be included in an application to the Secretary of State for the issue or renewal of a s.5 warrant. Apart from a description of the proposed interference and the measures to be taken to minimise intrusion, at the head of the list in both Codes is a requirement to specify "*the identity or identities, where known, of those who possess* [or use] *the* [equipment] *that is to be subject to the interference*" and "*sufficient information to identify the* [equipment] *which will be affected by the interference*" (the square bracketed parts are the changes from the Property Code to the draft E I Code).

41. We are entirely satisfied that Mr Jaffey's submissions have confused the property to be specified with the person or persons whose ownership or use of the equipment may assist in its identification. We do not accept his submission (Day 2/12) that the Secretary of State has to consider, by reference to each individual person who might use or own such equipment, whether CNE would be justified in each individual case. Questions of necessity and proportionality to be applied by the Secretary of State must relate to the foreseeable effect of the grant of such a warrant, and one of the matters to be considered is the effect and extent of the warrant in the light of the specification of the property in that warrant.

42. As originally enacted, s.5(2) authorised the Secretary of State to issue a warrant "*authorising the taking . . . of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State:*

(a) thinks it necessary for the action to be taken on the ground that it <u>is likely to be of substantial value in assisting</u> ... [our underlining]

(iii) GCHQ in carrying out any function which falls within Section 3(1)(a) and

(b) is satisfied that what the action seeks to achieve cannot reasonably be achieved by other means and

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

43. "*Specified*" must mean the same in relation to each action, property and wireless telegraphy. "*Wireless telegraphy*" as defined by s.11(e) of ISA meant

"*the emitting or receiving over paths which are not provided by any material substance constructed or arranged for that purpose, of electro magnetic energy or frequency not exceeding 3 million megacycles per second . . .*". (S.19(1) Wireless Telegraphy Act 1949).

44. Given the width of meaning contained in the words "*action*" and "w*ireless telegraphy*" and, at least potentially, in the word "*property*", *specified* cannot have meant anything more restrictive than 'adequately described'. The key purpose of specifying is to permit a person executing the warrant to know when it is executed that the action which he is to take and the property or wireless telegraphy with which he is to interfere is within the scope of the warrant.

45. It therefore follows that a warrant issued under s.5 as originally enacted was not required:

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

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

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

46. The amendment of s.7 in 2001 to add GCHQ cannot alter the meaning of s.5, which has, in all respects relevant to this Issue, remained unchanged.

47. In our judgment what is required is for the warrant to be as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable.

Issue 5: Scope of the Convention

48. Issue 5 is the question: Do Articles 8/10 apply to a complaint by reference to a s.7 authorisation? This issue only arose specifically in the course of the hearing, in which the Tribunal is of course being asked to decide pursuant to the List of Issues whether "*the regime which governs* [CNE] *is 'in accordance with the law' under Article 8(2) ECHR 'prescribed by law' under Article 10(2) ECHR"* (original Legal Issue 4).

49. S.7 applies, as is clear from its heading, to "*authorisation of acts outside the British Islands*". S.7 was not dealt with in the Property Code, and there is no power for the Secretary of State to issue Codes of Practice in relation to s.7, by

reference to s.71 of RIPA or at all (see paragraph 1.4). In that paragraph, and more specifically in paragraph 7.1 of the E I Code, it is stated that "*SIS and GCHQ should as a matter of policy apply the provisions of* [the] *code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands*". But there is a footnote to that paragraph which expressly says "*without prejudice as to arguments regarding the applicability of the ECHR*".

50. It was, in the event, common ground that, subject to Mr Jaffey's reserving his clients' position to be considered further if necessary in the ECtHR, there is a jurisdictional limit on the application of the ECHR, by virtue of Article 1, ECHR, which provides that "*the High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this Convention*". It was also common ground that, in the absence of any ECtHR authority, the Convention should not be interpreted more generously in favour of claimants than the ECtHR has been prepared to go, in circumstances where there is no right of appeal for the Government from the domestic courts to the ECtHR: see **R (Ullah) v Secretary of State for the Home Department** [2004] 2 AC 323 at para 20 per Lord Bingham.

51. Jurisdiction under the ECHR is accordingly territorial; and it is only in exceptional circumstances that extraterritorial jurisdiction arises (see **Bankovic v UK** [2007] 44 EHRR SE 5 and **Al-Skeini v UK** [2011] 53 EHRR 18 at para 131). As is made clear in **Bankovic** at paragraph 73, jurisdiction is not a doctrine of 'mere effects'.

52. There is thus no dispute between the parties that in ordinary circumstances there would be no jurisdiction by reference to Articles 8 or 10 with regard to the acts outside the British Islands which would be the subject of authorisation under s.7. Mr Eadie submitted that other circumstances would be exceptional. Mr Jaffey gave examples of circumstances which might engage those Articles: complainant in the jurisdiction but computer or information abroad, computer or phone brought back to the jurisdiction etc. But he accepted that in most cases where someone who is the subject of an authorisation granted under s.7 is abroad it was difficult to argue that such person is within the territorial scope of the Convention, and in any event that there would be a "*very limited number of circumstances*" in which there was going to be a breach of the Convention (Day 2/25). As is clear from the current Advance Training for Active Operations, disclosed in these proceedings, "*CNE operations must be authorised under ISA Section 5 or Section.7, depending whether the target computer or network is located within or outside the British Islands*".

53. Before fully accepting the consequences of the jurisdiction argument, which the Vice-President had put to him, Mr Jaffey appeared to argue (Day 1/161) that any s.7 authorisation prior to the introduction of the E I Code "*had to fall*" (Day 1/161), a submission which he later expressly clarified (Day 3/177). Both in that latter passage and earlier (Day 2/24-26) he appeared to agree in clear terms with Mr Eadie (Day 3/120) that the fact that there might be an individual claimant who might be able to claim a breach of Article 8/10 rights as a result of a s.7 authorisation would not lead to a conclusion that the s.7 regime as a whole could be argued to be non-compliant with Articles 8 or 10.

In any event we reserve for future consideration, if and when particular facts arise and the position of jurisdiction to challenge a s.7 warrant can be and has been fully argued, whether an individual complainant may be able to mount a claim. Even though Issue 5 was formulated as an agreed preliminary issue between the parties, it is clear to the Tribunal that, given the agreed difficult issues as to jurisdiction, we have an insufficient factual basis, assumed or otherwise, to reach any useful conclusion.

Issue 6: A s.5 warrant and Articles 8/10

54. We have concluded in respect of Issue 4 that a s.5 warrant is not as restricted as the Claimants have contended, by reference to construction of it at domestic law. Mr Jaffey submits that the Respondents are on a Morton's Fork, and that the wider the construction of s.5 for which they contend the more unlikely it is that there will be sufficient safeguards for the purposes of the ECHR. We can deal with this issue quite shortly.

55. Part of Mr Jaffey's case is again that, whereas s.7 provides for underlying approvals, as referred to in paragraph 35(ii) above, s.5 does not. But the essential question is, if an application for a warrant so specifies the property proposed to be covered by it as to enable a Secretary of State to be satisfied as to its legality, necessity and proportionality, and so that the property to be covered is objectively ascertainable (paragraph 47 above), whether a warrant so issued is in adequate compliance with the Convention.

56. As to Mr Jaffey's submissions in this regard:

i) He refers to **Malone v UK** [1985] 7 EHRR 14 as his foundation, but in that case, as he reminded us, the ECtHR made clear that "*in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations*" long before the present suite of statutory provisions. What the Court laid down as fundamental requirements, as set out in paragraphs 67 and 68 of the Judgment, is that "*there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities . . . A law which confers a discretion must indicate the scope of that discretion*".

ii) He naturally referred to **Weber** and **Saravia v Germany** [2008] 46 EHRR SE5, which we addressed in detail in **Liberty/Privacy (No.1)**, and in paragraph 33 of that judgment we set out the "**Weber** requirements", numbering them from 1 to 6 for convenience:

> "95. *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."

57. In **R.E. v UK**, the ECtHR was satisfied, with regard to the surveillance provisions there referred to, so far as concerned **Weber** (1) and (2) at paragraph 136 of its Judgment, and so far as duration is concerned gave approval in paragraph 137. Duration of the s.5 warrant is limited by s.6, to which no specific criticisms have been addressed.

58. In **Weber** itself, a broad and untargeted warrant, similar to a warrant under s.8(4) of RIPA - a far broader and less *specified* warrant than the s.5 warrant which we are here considering - was found to comply with the Convention.

59. We are satisfied in this case that a s.5 warrant which accords with the criteria of specification which we have set out at paragraph 47 above complies with **Weber** (1) to (3), namely in regard to the circumstances, the definition of the categories of people/property and duration, and consequently with Articles 8 and 10 in that regard. We deal with **Weber** (4) to (6) below.

Issue 7: Bulk CNE

60. Issue 7 relates to the absence of a similar certificate to that in s.16 of RIPA in relation to CNE. It arises from the matters in (e) in the original paragraph 6 of the List of Issues, set out in paragraph 9 above, which were the subject of NCND by the Respondents. There are two specific complaints which are made:

i) That, unlike in the case of a s.8(4) warrant under RIPA, where communications are intercepted in bulk and subsequently accessed for examination, there is no provision, in the event of this occurring pursuant to CNE, for 'filtering': i.e. as in s.16(1) and (3) of RIPA for intercept to be read, looked at or listened to only by reference to a certificate that the examination of material selected is necessary for one of the statutory purposes. S.16 is what was referred to in **Liberty/Privacy (No.1)** (paragraph 103) as the provision which did the '*heavy lifting*'.

ii) That there is no special protection, if information is obtained in bulk through the use of CNE, for those persons *known to be for the time being in the British Islands*, as in s.16(2)(3) and (5) of RIPA. Such a scenario is in fact addressed in the E I Code at paragraph 7.4 (relating to a s.7 warrant) which reads:

"*7.4 If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation*

> *authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).*"

David Anderson in his Report refers to this paragraph of the E I Code, and comments, at paragraph 6.33:

> "*It does not elaborate on what factors should be taken into account in the course of that 'consideration'.*"

61. As for the latter point (ii), Mr Eadie submits, and we accept, that, provided that the matter is indeed considered, as is required by paragraph 7.4, such an issue is simply one of the matters which are required to be brought before a Secretary of State, pursuant to his obligation to consider alternative and/or less intrusive measures, rather than, as Mr Jaffey submitted, that this is part of an attempt to circumvent the statutory scheme under s.8(4).

62. Both aspects of Mr Jaffey's complaints appear to have been taken up in the IP Bill. Under the heading "*BULK POWERS*" in the accompanying Guide, it is stated, at paragraph 42, that where the content of a UK person's data, acquired under bulk interception and bulk equipment interference powers, is to be examined, a targeted interception or equipment interference warrant will need to be obtained. As for the question of presence in the British Islands, it is specifically provided in draft clause 147, within the Chapter dealing with "*Bulk Equipment Interference Warrants*", namely by clause 147(4), that there is to be a similar safeguard to that in s.16 of RIPA in relation to the selection of material for examination referable to an individual known to be in the British Islands at the time.

63. It seems to us clear that these criticisms are likely primarily to relate to Bulk CNE carried out, if it is carried out at all, pursuant to a s.7 authorisation (hence paragraph 7.4 of the E I Code). Mr Jaffey's own example was of the hacking of a large internet service provider in a foreign country, and the diversion of all of the data to GCHQ, instead of intercepting that material "*over a pipe*" which might be encrypted, so as to render access by ordinary bulk interception difficult if not impossible. As with Issue 5, Mr Jaffey specifically accepted (Day 2/46) that, if Bulk CNE were taking place, and if, prior to any changes such as discussed above, there were to be insufficient safeguards in place, that does not render the whole CNE scheme unlawful. As with Issue 5, we reserve for consideration, on particular facts and when questions of jurisdiction are examined, whether an individual complainant might be able to mount a claim.

Issue 8: S.5 post-February 2015 (**Weber (**4) to (6)

64. Issue 8 is: Whether the s.5 regime is compliant with the Convention since February 2015. We now address **Weber** (4) to (6). The E I Code applies to both s.5 and s.7 (see paragraph 49 above), and, as Mr Jaffey accepted, the Respondents, having publicly accepted that they are acting and will act in accordance with the draft Code, are as a matter of public law bound by the Code both in relation to s.5, during the period prior to its being finally approved by Parliament (see paragraph 7 above), and s.7. However in the light of our conclusions in respect of Issue 5, we now address only the question of s.5, though in relation to this Issue the answer would be the same in respect of s.7.

65. We do not need to repeat all of what we said in **Liberty/Privacy (No.1)** (in particular at paragraphs 38-41) by way of summary of the ECtHR jurisprudence. It suffices to cite what we said at paragraph 41(d), namely:

> "*It is in our judgment sufficient that:*
>
> *i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it . . .*
>
> *ii) They are subject to proper oversight.*"

The oversight relevant to this issue by the Intelligence Services Commissioner seems to us to have been admirable in its dedication to raising any questions of concern.

66. In addition to the E I Code, in November 2015 there was disclosure during these proceedings of *below the waterline arrangements* applicable to GCHQ, whose existence is highlighted in the E I Code (e.g. at paragraph 64) and in statute, as canvassed in our judgments in **Liberty/Privacy No.1** and **No.2**. Insofar as those *arrangements* add something new which had not been previously signposted, and which would not therefore have been *accessible/foreseeable*, then any unlawfulness in relation to the published code would only have been made good by the publication of such *arrangements* in November. Mr Jaffey has submitted that the *arrangements* should have been disclosed earlier, but, as will appear, we do not conclude that the content of those *arrangements* as now disclosed adds anything material to the previously published Code.

67. There has been no material addition to ECtHR jurisprudence since **Liberty/Privacy** with the exception of **R.E. v UK**, to which we shall return below, and in which (particularly at paragraph 133) the Court repeated the same principles in the context of national security.

68. It is common ground that compliance with the Convention can be addressed by reference to the **Weber** requirements, and in this regard specifically by **Weber** (4) to (6). The significant paragraphs of the E I Code relating to **Weber** (4) to (6) are in Sections 5 and 6, which are attached as Appendix II to

this judgment, though Weber (6) may not be directly applicable to the use of CNE so far as it consists of 'implants'. We have attached the paragraphs in the form in which they were put before Parliament in November 2015. Although there have been some changes in the draft E I Code during the period of public consultation, and the parties helpfully provided us with tracked changes to explain them, there were none which appeared to us to be material: Mr Jaffey pointed to a number of changes (two in the Sections included in Appendix 2, one in paragraph 6.2 and one in 6.5) of the words *must* to *should*, but he was not able to identify to us, and nor can we see, any material difference in that regard. There are then the *below the waterline arrangements* which have been disclosed from GCHQ's policies, relating to storage of and access to data, and handling/disclosing/sharing of data, obtained by CNE operations. Neither Mr Eadie nor Mr Jaffey suggested that there were any apparent lacunae or alleged inadequacies in the Code which were made good by the disclosure of these *arrangements*.

69. There were very limited criticisms made by Mr Jaffey, in the context of **Weber** (4) to (6), of the E I Code (even without the supplementary *arrangements*):

i) He was critical of the apparent lack of provision for record keeping in relation to intrusions pursuant to s.7, but, quite apart from the fact that this related to s.7 and not to s.5, in fact it is clear that, as indeed he accepted, a combination of paragraphs 5.1 and 7.2 of the E I Code does require the keeping of records in relation to "*the details of what equipment interference has occurred*".

ii) He described as "*Delphic*" a reference in Mr Martin's witness statement to the nature of a recommendation by the Intelligence Services Commissioner with regard to a s.5 record, but accepted the explanation provided by Mr Eadie during the course of his submissions: Day 3/74.

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

Issue 9: S.5 prior to February 2015

71. The issue is: Did the s.5 regime prior to February 2015 accord with the Convention (it is accepted that, as set out in paragraph 49 above, the Property Code did not apply to s.7)?

72. This is obviously a more difficult question, because, by definition, if the publication of the E I Code in February 2015 improved the position, and made sufficiently public the arrangements which govern the use by the Respondents of their powers, the published arrangements prior to February must have been

inferior. Mr Eadie emphasises that the Tribunal, and indeed any court, should not discourage improvement by immediately concluding that what was in existence prior to an improvement was defective. He obviously accepts our conclusion at paragraph 23 of **Liberty/Privacy No.2** that, before the disclosures prior to and in our judgment in that case, the regime governing information sharing under Prism had been unlawful, but he submits, as is the case, that there had been effectively no disclosure at all prior to that of the existence of any arrangements, adequate or otherwise.

73. The question for us is, as it was for the ECtHR in **Liberty v UK** [2008] 48 EHRR 1 (at paragraph 69), whether at the time the regime complied, and that time in these proceedings is, pursuant to the agreed List of Issues at paragraph 4(d), 1 August 2009. The Property Code was in existence throughout the period from August 2009 to February 2015 and did not materially change, and so we have addressed the most recent version (2014).

74. There are underlying issues:

i) It was not, at any rate with any great force, sought to be argued by Mr Jaffey that the position was any different in relation to **Weber** (1) to (3) prior to and subsequent to February 2015, and we are satisfied that our conclusions in Issue 6 above apply prior to February 2015, and we shall address for the purposes of this Issue only **Weber** (4) to (6).

ii) It was common ground before us that **Weber** (1) to (6) constitute a minimum to be complied with, but that there are other factors to consider such as:

a) The existence and standard of oversight. It is entirely clear to us that both sides have relied upon his Reports, and that the oversight by the Intelligence Services Commissioner has been of great value.

b) The existence of sufficiently signposted underlying *arrangements*, which are adequate to control arbitrary action by the Respondents. It is important to bear in mind, for example, that the Tribunal concluded in **Liberty/Privacy No.1** that the s.8(4) regime complied with the Convention, after taking into account the *arrangements*, which we concluded had been adequately signposted prior to any further disclosures by the Respondent (e.g. paragraph 140). This did not involve or require disclosure of the detail of those *arrangements*.

iii) **R.E. v UK** requires to be addressed specifically, as the only relevant ECtHR decision since **Liberty/Privacy**. The Court was addressing the Property Code (there called the "Revised Code"), and contrasting it with the Interception of Communications Code of Practice ("the Interception Code"), which the ECtHR had approved in **Kennedy v UK** [2011] 52 EHRR 4. The case before it concerned the issue of the safeguarding of legally and professionally privileged ("LPP") communications in relation to covert surveillance. The Court

concluded that **Weber** (1) to (3) were satisfied, but that **Weber** (4) to (6) were not. We shall need to address that conclusion, unfavourable to the Respondents, by the Court.

75. The material provisions for consideration in respect of the period from August 2009 to February 2015 are as follows:

i) The statutory provision in relation to GCHQ, which is obviously fundamental. This appears in s.4 of ISA.

> *"4 The Director of GCHQ.*
>
> *(1) The operations of GCHQ shall continue to be under the control of a Director appointed by the Secretary of State.*
>
> *(2) The Director shall be responsible for the efficiency of GCHQ and it shall be his duty to ensure—*
>
> *(a) that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings; and*
>
> *(b) that GCHQ does not take any action to further the interests of any United Kingdom political party.*
>
> . . .
>
> *(4) The Director shall make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State and may at any time report to either of them on any matter relating to its work.*"

There is a cross reference to s.4 in s.5(2)(c) of ISA, set out in paragraph 4 above together with s.6, which is also relevant.

ii) The other related statutory provisions set out in paragraph 6(ii), (iii) and (iv) above: disclosure or use by an employee of GCHQ of information in breach of a relevant *arrangement* within s.4(2)(a) of the ISA above set out would constitute a criminal offence pursuant to the OSA.

iii) The Property Code, being the published *arrangements*. Relevant to **Weber** (4) to (6) are:

> "*8.3 The following information relating to all authorisations for property interference should be centrally retrievable for at least three years:*

• the time and date when an authorisation is given;

• whether an authorisation is in written or oral form;

• the time and date when it was notified to a Surveillance Commissioner, if applicable;

• the time and date when the Surveillance Commissioner notified his approval (where appropriate);

• every occasion when entry on or interference with property or with wireless telegraphy has occurred;

• the result of periodic reviews of the authorisation;

• the date of every renewal; and

• the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy.

. . .

9.3 Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or 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.

. . .

9.7 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 1989 Act and the 1994 Act."

76. There are then the *under the waterline arrangements*. In this regard we refer to paragraphs 42 to 44 of the Tribunal's judgment in **Liberty/Privacy No.1**, the relevant cross-references for the purposes of this case being to paragraph 18(ix) and (xi) of that Judgment. In addition to the statutory provisions we have referred to in paragraph 75 above, there is the reference in paragraph 9.3 of the Property Code to *arrangements* and *codes of practice*. The arrangements so signposted are summarised in paragraph 99ZK-99ZR of the

Respondents' Open Response as follows (underlining in the original signifies the existence of gisting):

> *"Storage of and access to data*
>
> *99ZK. GCHQ also has policies for storage of and access to data obtained by CNE.*
>
> *99ZL. The section of the Compliance Guide concerning "Review and Retention" states that GCHQ treats "all operational data" (i.e. including that obtained by CNE) as if it were obtained under RIPA. It sets out GCHQ's arrangements for minimising retention of data in accordance with RIPA safeguards. This is achieved by setting default maximum limits for storage of operational data.*
>
> *99ZM. In addition GCHQ has a separate policy specifically concerning data storage and access. It defines different categories of data, and importantly ascribes specific periods for which different categories of data may he kept, as well as explaining how different categories of CNE data relate to the categories of operational data set out in the Compliance Guide.*
>
> *99ZN. Where CNE analysts identify material as being of use for longer periods than the stipulated limits, it can be retained for longer, subject to justification according to specific criteria.*
>
> *99Z0. Access to data is also subject to strict safeguards, which are set out in the Compliance Guide. CNE content may be accessed by intelligence analysts, but they must first demonstrate that such access is necessary and proportionate by completing a Human Rights Act ("HRA") justification. HRA justifications are recorded and made available for audit. CNE technical data relating to the conduct of CNE operations may only be accessed by a team of trained operators responsible for planning and running such operations.*
>
> *99ZP. GCHQ's policy on storage of and access to data also requires GCHQ analysts who are not in the CNE operational unit to justify access to CNE data on ECHR grounds (particularly*

necessity and proportionality). The justification must be recorded and available for audit.

Handling/disclosure/sharing of data obtained by CNE operations

99ZQ. Pursuant to GCHQ's Compliance Guide, the position is that all operational material is handled, disclosed and shared as though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

99ZR. The general rules, as set out in the Compliance Guide and the intelligence Sharing and Release Policy which apply to the handling of operational material include, inter alia, a requirement for mandatory training on operational legalities and detailed rules on the disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them.

a) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report.

b) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the "Communications Containing Confidential Information" section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators) GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate."

77. This is a very full picture of the guidelines under which GCHQ is required to operate, and we are satisfied that they would be adequate, in the context of the

interests of national security, to impose the necessary discipline on GCHQ, and give adequate protection against arbitrary power: further there is, as we have been satisfied, adequate oversight of GCHQ's compliance by the Intelligence Services Commissioner.

78. The nub of the problem arises in two respects, both emphasised by Mr Jaffey:

i) The impact of the fact that until February 2015, i.e. throughout the period we are addressing, it was not admitted by the Respondent that GCHQ carried out CNE;

ii) The impact of the decision of **R.E. v UK,** in relation to the consideration by the ECtHR.

We will deal with the second submission first.

79. It is important to bear in mind that, as set out in paragraph 74(iii) above, the Court in **R.E. v UK** was addressing a specific and different question, the matter of adequate protection for LPP communications in respect of covert surveillance. We deal ourselves with LPP as a separate topic in Issue 10 below, and we are not concerned with it in our present considerations. We set out the conclusions of the Court in **R.E. v UK** in relation to the Revised Code (the Property Code) and **Weber** (4) to (6), after it has recorded its conclusion that it was satisfied in relation to **Weber** (1) and (2) (in paragraph 136) and **Weber** (3) (in paragraph 137):

> "*138. In contrast, fewer details concerning the procedures to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or the tapes destroyed are provided in Part II of RIPA and/or the Revised Code. Although material obtained by directed or intrusive surveillance can normally be used in criminal proceedings and law enforcement investigations, paragraph 4.23 of the Revised Code makes it clear that material subject to legal privilege which has been deliberately acquired cannot be so used (see paragraph 75 above). Certain other safeguards are included in Chapter 4 of the Revised Code with regard to the retention and dissemination of material subject to legal privilege (see paragraph 75 above). Paragraph 4.25 of the Revised Code provides that where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection. The material should be made available during the inspection if requested. Furthermore, where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, Paragraph 4.26*

of the Revised Code states that advice should be sought from a legal advisor before any further dissemination takes place; the retention or dissemination of legally privileged material should be accompanied by a clear warning that it is subject to legal privilege; it should be safeguarded by taking "reasonable steps" to ensure there is no possibility of it becoming available, or it contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings; and finally, any dissemination to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

139. These provisions, although containing some significant safeguards to protect the interests of persons affected by the surveillance of legal consultations, are to be contrasted with the more detailed provisions in Part I of RIPA and the Interception of Communications Code of Practice, which the Court approved in Kennedy (cited above, §§ 42 – 49). In particular, in relation to intercepted material there are provisions in Part I and the Code of Practice limiting the number of persons to whom the material is made available and restricting the extent to which it is disclosed and copied; imposing a broad duty on those involved in interception to keep everything in the intercepted material secret; prohibiting disclosure to persons who do not hold the necessary security clearance and to persons who do not "need to know" about the material; criminalising the disclosure of intercept material with an offence punishable by up to five years' imprisonment; requiring intercepted material to be stored securely; and requiring that intercepted material be securely destroyed as soon as it is no longer required for any of the authorised purposes.

140. Paragraph 9.3 of the Revised Code does provide that each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through directed or intrusive surveillance. In the present case the relevant arrangements are contained in the PSNI Service Procedure on Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material. The Administrative Court accepted that taking together the 2010 Order, the Revised Code and the PSNI Service Procedure Implementing Code, the arrangements in place for the use, retention and destruction of retained material in the context of legal consultations was compliant with the Article 8 rights of

persons in custody. However, the Service Procedure was only implemented on 22 June 2010. It was therefore not in force during the applicant's detention in May 2010.

141. The Court has noted the statement of the Government in their observations that only one intrusive surveillance order had been granted up till then in the three years since the 2010 Order (introducing the Revised Code) had come into force in April 2010 (see paragraphs 11 and 12 above). Nevertheless, in the absence of the "arrangements" anticipated by the covert surveillance regime, the Court, sharing the concerns of Lord Phillips and Lord Neuberger in the House of Lords in this regard (see paragraphs 36 – 37 above) is not satisfied that the provisions in Part II of RIPA and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed provide sufficient safeguards for the protection of the material obtained by covert surveillance.

142. Consequently, the Court considers that, to this extent, during the relevant period of the applicant's detention (4 – 6 May 2010 – see paragraphs 18 – 20 above), the impugned surveillance measures, insofar as they may have been applied to him, did not meet the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law."

80. It seems to us entirely clear that they were addressing the adequacy of the Property Code (as compared with the Interception Code) in respect of LPP communications, in relation to which (as discussed in Issue 10) the Government has previously conceded before this Tribunal that the regime established by and for the Intelligence Services was not compliant with the Convention (**Belhadj** [2015] UKIP TRIB 13_132-8 of 29 April 2015). When the ECtHR addressed, in the cited paragraph 139 above, the benefits of the Interception Code, it is plain to us that they were doing so not in respect of **Weber** (4) to (6) generally, but in respect of the way in which the Interception Code gave improved safeguards by protecting "*the interests of persons affected by the surveillance of legal consultations*". The Court did not address specifically, and reach conclusions as to, whether the Property Code was inadequate (other than in respect of LPP) to comply with **Weber** (4) to (6) in the light of:

(i) the statutory obligations of and upon GCHQ referred to in paragraph 75 (i) and (ii) above (very much more significant than those imposed upon the Police):

(ii) the provisions of paragraph 9.3 and 9.7 of the Code:

(iii) the *under the waterline arrangements* set out in paragraph 76 above, which we are satisfied were adequately signposted:

(iv) the oversight by the Intelligence Services Commissioner of GCHQ's compliance with their obligations.

Taken together, these are safeguards designed to prevent any arbitrary exercise of the powers to conduct CNE. But none of the safeguards would have been an answer to a system concluded (and now conceded) to have been inadequate in respect of its protection of LPP communications.

81. As to the first submission, as referred to in paragraph 78 (i) above, it is clear that prior to February 2015 there was no admission that property interference by GCHQ (governed by the Property Code) extended to CNE by the use of a s.5 warrant (or *a fortiori* a s.7 authorisation). Nevertheless it was quite clear that at least since 1994 the powers of GCHQ have extended to computer interference (under s.3 of ISA). It was thus apparent in the public domain that there was likely to be interference with computers, 'hacking' being an ever more familiar activity, namely interference with property by GCHQ (and see in particular the 1990 Hansard references in paragraph 18 (iii) above), and that if it occurred it would be covered by the Property Code. Use of it was thus foreseeable, even if the precise form of it and the existence of its use was not admitted.

82. The question is whether we are satisfied that there was, prior to February 2015, adequate protection from arbitrary interference. If there was inadequacy within the Property Code, as compared with the EIC, we do not conclude that the inadequacy was in the circumstances such as to constitute a contravention of Articles 8/10. Compliance with **Weber** (4) to (6) will in our judgment mean the provision, particularly in a national security context, of as much information as can be provided without material risk to national security. In our judgment, not least because of the consequences of a conclusion of unlawfulness simply by virtue of a perceived procedural insufficiency, a conclusion that procedural requirements or the publication of them can be improved (i) does not have the necessary consequence that there has prior thereto been insufficient compliance with **Weber** (4) to (6) and (ii) does not constitute such a material non-compliance as to create a contravention of Article 8. This Tribunal sees it as an important by-product of the exercise of its statutory function to encourage continuing improvement in the procedures adopted by the Intelligence Agencies and their publication (and indeed such improvement took place as a consequence of our Judgments in **Liberty/Privacy No.1**, **Liberty/Privacy No.2** and **Belhadj**), but it does not conclude that it is necessary, every time an inadequacy, particularly an inadequate publication, is identified, to conclude that that renders all previous conduct by the Respondents unlawful. The E I Code is plainly a step forward by the Respondents, which this Tribunal welcomes: taking the Property Code together with the other safeguards which we have set out in paragraph 80 above, we are satisfied that there was prior to that step adequate protection from arbitrary interference.

83. We accordingly resolve Issue 9 in favour of the Respondent. The s.5 regime prior to February 2015 was compliant with the Convention.

Issue 10 Legal and Professional Privilege

84. Issue 10 is: Does the system relating to LPP communications derived from CNE since February 2015 comply with the Convention? Mr Jaffey raised briefly at one stage the question of journalistic sources, but that forms an entirely separate topic, with which this judgment does not deal. The Respondents accepted in **Belhadj** 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. This Issue 10 therefore relates only to the period since February 2015 and whether, in relation to LPP, the E I Code has remedied the problem. Mr Jaffey raised only three points by way of continuing criticism, and in the event all of them have become moot so far as any continuing problem is concerned.

85. The first related to GCHQ's definition of legal and professional privilege, which had previously appeared not to include litigation privilege. Mr Jaffey accepts that this has now been made good by the adoption in the E I Code of a definition of privilege analogous to that in the Police Act, which does not exclude litigation privilege.

86. The second criticism related to the fact that the Respondents have said that they were establishing appropriate 'Chinese walls' which would satisfy Mr Jaffey's concerns but did not yet appear to have done so. According to Mr Martin's second statement at paragraph 18, the practice, now described in a document headed "Summary of GCHQ Policy on Handling Material Derived from the Interception of Communications of Individuals Engaged on Legal Proceedings where HMG has an Interest" was still awaiting formal approval. Mr Eadie told us on instructions that the policy had in fact been implemented while still in draft in April 2015, but accepted that nevertheless it had not yet been approved, albeit imminently was to be so. He also referred to paragraph 3.19 of the E I Code, by which the detailed guidance in paragraphs 3.1-3.18, with which Mr Jaffey takes no exception, "*takes precedence over any contrary content of an agency's internal advice or guidance*". Nevertheless we have now been supplied since the hearing with confirmation that this policy was approved, in November 2015.

87. The third problem was that of metadata, which could attract LPP by reference to communications with lawyers, even without their content. There was no dispute between Counsel that metadata might attract LPP. There was no specific mention of metadata in the E I Code, although that of itself would not be a problem. What is a problem is that there is an apparent express exclusion from potentially LPP material of metadata in an internal GCHQ document called "Summary of GCHQ LPP and Sensitive Communications Policy". Because of the lack of mention of metadata in the E I Code, this would not benefit from the 'override' of clause 3.19, and plainly there has been the risk of somebody incorrectly relying upon such guidance. Mr Eadie told us that this guidance would be corrected, and since the hearing a copy of such corrective policy has

been supplied to us, attached as Appendix III: again the underlining denotes gisting.

88. Even without such corrections, Mr Jaffey made clear that none of his criticisms would result in this case in the whole system being unlawful, but it is accepted that there might on the facts (including the facts relating to these Claimants) be a case in which LPP communications have been inappropriately dealt with by virtue of the absence of accurate guidance or policy at the time, and thus amount to a breach of Article 8. There is no need for us to give any specific conclusion in relation to this issue, the discussion of which has once again proved the value of these inter partes proceedings.

Conclusion

89. Our conclusions in relation to the above Issues, where material, are consequently as follows.

(i) Issue 1: An act (CNE) which would be an offence under s.3 of the CMA is made lawful by a s.5 warrant or s.7 authorisation, and the amendment of s.10 CMA was simply confirmatory of that fact.

(ii) Issue 2: An act abroad pursuant to ss.5 or 7 of the ISA which would otherwise be an offence under ss.1 and/or 3 of the CMA would not be unlawful.

(iii) Issue 3: The power under s.5 of ISA to authorise interference with *property* encompasses intangible property.

(iv) Issue 4: A s.5 warrant is lawful if it is as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable, and it need not be defined by reference to named or identified individuals.

(v) Issue 5: There might be circumstances in which an individual claimant might be able to claim a breach of Article 8/10 rights as a result of a s.7 authorisation, but that does not lead to a conclusion that the s.7 regime is non-compliant with Articles 8 or 10.

(vi) Issue 6: A s.5 warrant which accords with the criteria of specification referred to in Issue 4 complies with the safeguards referred to in **Weber** (1) to (3), and consequently with Articles 8 and 10 in that regard.

(vii) Issue 7: If information were obtained in bulk through the use of CNE, there might be circumstances in which an individual complainant might be able to mount a claim, but in principle CNE is lawful.

(viii) Issue 8: The s.5 regime since February 2015 is compliant with Articles 8/10.

(ix) Issue 9: The s.5 regime prior to February 2015 was compliant with Articles 8/10.

(x) Issue 10: So far as concerns the adequacy of dealing with LPP, the CNE regime has been compliant with the Convention since February 2015.

90. The use of CNE by GCHQ, now avowed, has obviously raised a number of serious questions, which we have done our best to resolve in this Judgment. Plainly it again emphasises the requirement for a balance to be drawn between the urgent need of the Intelligence Agencies to safeguard the public and the protection of an individual's privacy and/or freedom of expression. We are satisfied that with the new E I Code, and whatever the outcome of Parliamentary consideration of the IP Bill, a proper balance is being struck in regard to the matters we have been asked to consider.

APPENDIX I

SCHEDULE

LEGAL ISSUES

Domestic law

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?

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?

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?

ECHR

4. 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?

5. Specifically:

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?

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?

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?

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?

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

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

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

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

APPENDIX II

Equipment Interference Code of Practice

As approved S.I. 2016 no.38

5. Keeping of records

Centrally retrievable records of warrants

5.1 The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- All applications made for warrants and for renewals of warrants:
- the date when a warrant is given;
- whether a warrant is approved under urgency procedures;
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal; and
- the date when any instruction was given by the Secretary of State to cease the equipment interference.

6. Handling of information and safeguards

Overview

6.1 This chapter provides further guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant. This information may include communications content and communications data as defined in section 21 of the 2000 Act.

6.2 The Intelligence Services must ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts[2]), the Data Protection Act 1998 and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with this legal framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse.

---

2 All information obtained by equipment interference must be handled in accordance with arrangements made under section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act (and pursuant to sections 5(2)(c) and 7(3)(c) of the 1994 Act).

Use of information as evidence

6.3 Subject to the provisions in chapter 3 of this code, information obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the 1998 Act.

Handling information obtained by equipment interference

6.4 Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which must be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference. Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.

6.5 These arrangements should be made available to the Intelligence Services Commissioner. The arrangements must ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements must be reported to the Intelligence Services Commissioner as agreed with him.

Dissemination of information

6.6 The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.

6.7 The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed. In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.

Copying

6.8 Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify

themselves as the product of an equipment interference operation. The restrictions must be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.

Storage

6.9 Information obtained by equipment interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.

Destruction

6.10 Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, must be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Personnel security

6.11 In accordance with the need-to-know principle, each of the Intelligence Services must ensure that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance. Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance.

Appendix III

Reporting LLP

Legally privileged communications

The GCHQ Compliance Guide explains that the RIPA Interception of Communications Code of Practice stipulates that greater regard should be had for privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved. This means that there are certain categories of communication where a particular high threshold of proportionality must be applied to the release of the content, because the content of the communication would ordinarily be considered confidential (in the common sense of the word) or otherwise privileged. These categories are:

-Legally privileged communications;
-Personal information held in confidence relating to physical or mental health;
-Personal information held in confidence relating to spiritual counselling:
-Confidential journalistic material;
-Confidential constituent information

Legal Professional Privilege (LPP) broadly falls into two categories.

-**legal advice privilege** which attaches to communications between a professional legal adviser, acting as such, and their client where the communications are made confidentially for the purpose of seeking or providing legal advice.

-**litigation privilege** which attaches to communications between the client and his legal adviser or agent, or between one of them and a third party, if such communications come into existence for the sole or dominant purpose of either seeking or providing legal advice with regard to litigation or collecting evidence in respect of litigation. This second category is wider than the first since it is possible for
litigation privilege to attach to communications other than those directly between a lawyer and their client, *i.e.* privilege can attach to communications between a lawyer and a third party where such communications are in connection with legal proceedings.

The concept of LPP applies to:

- The content of communications that fall into one of the categories above, and

- Exceptionally, some communications data (*i.e.* 'events' or the fact of a communication),

The purpose of LPP is to ensure that individuals are able to consult a lawyer in confidence without fear that what passes between them will later be used against
them in court and it is therefore fundamental to the right to a fair trial and the rule of law. Intelligence material subject to LPP cannot be released to a customer who may
be a party to any legal case to which the material relates, because this would give
that customer an unfair litigation advantage (it being a basic principle that litigants cannot be required to reveal privileged material to either their opponents or the

court in a given piece of litigation). However, communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably) are unlikely to be protected by LPP. For more details contact the Disclosure Policy team.

The judgment as to whether it is necessary and proportionate to include information subject to LPP in the release of intelligence material by GCHQ must take account of the particular sensitivity of such information and any associated risks. It is likely that any release of material protected by LPP that is deemed both necessary [and] proportionate will be to a more limited readership limited and possibly more highly classified than would otherwise be the case. The judgment of necessity and proportionality in these cases is reserved to Mission Policy, and all reporting containing anything that you believe may be covered by LPP must be submitted for checking. For the sake of simplicity, in order to ensure that all intelligence material containing potentially LPP information is submitted and assessed, reports featuring the following types of intelligence must be submitted for checking before issue:

- Content and/or communications data ('events') relating to (including instances where a target has been in contact with) lawyers, legal advisers, solicitors, attorneys, or any other member of the legal profession, or content that includes legal advice, regardless of the profession of the communicant.

The sensitivity of reporting LPP information is not mitigated by disguising or removing the identity or occupation of the communicant. But neither is there a 'ban' on identifying or reporting such material – it may well be necessary and proportionate to report such information to certain circumstances. The checking process is designed to determine this. If Mission Policy considers it proportionate in a particular case to release intelligence based on communications that attract legal privilege, the reporter will be instructed to apply the following rubric to the report:

This report contains material that may be subject to legal professional privilege, and onward dissemination/Action On is not to be taken without reverting to GCHQ.