Case No. IPT 14/85/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

Case No. IPT 14/120-126/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

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

Claimants

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

THE RESPONDENTS' RE-RE-AMENDED OPEN RESPONSE

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

INTRODUCTION

1. The two Claims overlap substantially. For convenience, the Respondents are filing a single Open Response to both Claims.

2. This Open Response:

   (a) Summarises the need for the "neither confirm nor deny" policy, and explains its operation in the present case pp2-3.

   (b) Addresses the Tribunal's procedural regime, insofar as is relevant to the present Claims pp3-5.

   (c) Addresses the complaints made in the proceedings and in particular :

      (a) sets out the Respondents' open position on the factual allegations made pp5-8;

      (b) sets out the relevant domestic legal regime ("the Equipment Interference Regime") pp8-44;

      (c) identifies the pure issue of law which is suitable for determination at a public *inter partes* hearing ("a Legal Issues Hearing") p44; and

      (d) sets out the Respondents' position on that pure issue of law, p45-54.

   (d) Suggests directions for the future management of these two Claims (p54).

3. The Respondents' overall position is that the Equipment Interference Regime is compatible with Arts 8, 10 and (if it is engaged by the Greennet complaint) Article 1 of the First Protocol to the ECHR. The Claims should therefore be dismissed.

THE "NEITHER CONFIRM NOR DENY" POLICY, AND ITS OPERATION IN THE PRESENT CASE

4. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See *e.g. Attorney General v. Guardian Newspapers Ltd (No.2)* [1990] 1 AC 109, *per* Lord Griffiths at 269F.

5. As a result, the mere fact that the Intelligence Services are carrying out an investigation or operation in relation to say, a terrorist group or hold information on a suspected terrorist will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or

continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.

6. In addition, an appropriate degree of secrecy must be maintained as regards the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.

7. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.

8. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (*i.e.* "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.

9. It has thus been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government.[1] That long-standing policy is applied in this Open Response.

THE TRIBUNAL'S PROCEDURAL REGIME[2]

10. The Tribunal's procedure is governed by ss. 67-69 of RIPA and the Investigatory Powers Tribunal Rules 2000, SI 2000/2665 ("the Rules"), made under s. 69.

11. In §173 of the Procedural Ruling of 22 January 2003 in IPT/01/62 and IPT/01/77 ("the Procedural Ruling") the Tribunal concluded that r. 9(6) of the Rules[3] was *ultra vires* the rule-making power in s. 69 of RIPA. Further, the

[1] Such a confirmation would only be given in exceptional circumstances – for example, on the basis either that there were some compelling countervailing public interest in departing from the neither confirm nor deny principle that clearly outweighed the public interest in protecting national security (or on balance promoted the public interest in protecting national security).

[2] The Tribunal's jurisdiction and remedial powers are addressed below.

[3] R. 9(6) provides:

"*The Tribunal's proceedings, including any oral hearing, shall be conducted in private*."

Tribunal held that:

(a) "purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of sensitive information" should be heard by the Tribunal in public (Procedural Ruling, §172); and

(b) the Tribunal's reasons for its ruling on any "pure questions of law" (§195) that are raised at such a hearing may be published without infringing either r. 13 of the Rules or s. 68(4) of RIPA[4] (Procedural Ruling, §§190-191).

12. It follows that, where necessary, the Tribunal may hold a Legal Issues Hearing to consider any relevant (and disputed) pure issues of law,[5] and may subsequently publish its rulings (with its reasoning) on such issues.

13. The Tribunal also concluded in the Procedural Ruling that, with the exception of r. 9(6), the Rules are valid and binding (§148). It follows from this conclusion, and from r. 6(2)-(5) of the Rules, that - prior to the determination of a claim[6] - the Tribunal cannot disclose to a claimant anything that a respondent has decided should only be disclosed to the Tribunal, and similarly cannot order a respondent to make such disclosure itself.

14. The overall effect of the Procedural Ruling is thus that:

(a) where necessary, the Tribunal first holds a Legal Issues Hearing to determine such relevant pure issues of law as are in dispute between the parties, and publishes its rulings (with reasons) on those pure issues of law;

(b) the Tribunal then investigates the claim in closed session; and

(c) as necessary,[7] the Tribunal applies its rulings on the pure issues of law to the facts that it has found following its closed session investigation of the claim.

15. This was the approach taken in the two joined cases which gave rise to the

[4] The effect of r. 13 and s. 68(4) is in essence that if the claim is dismissed then the Tribunal may only give to the claimant a statement that "*no determination has been made in his favour*", but that if the claim is upheld then the Tribunal may, subject to r. 6(1), provide a summary of its determination, including any findings of fact.

[5] As the Tribunal confirmed in the subsequent case of *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH), 26 February 2008, at §5, the pure issues of law can as necessary be considered on the basis of hypothetical facts.

[6] As noted in footnote 5 above, the Tribunal has power - subject to r. 6(1) - to provide a summary of its determination, including any findings of fact, in the event that the overall claim is upheld.

[7] Following its investigation the Tribunal may *e.g.* find that the respondents have not in fact undertaken any activities in relation to a claimant, with the result that the claim will be dismissed without the need to apply the rulings on the pure issues of law to any specific factual findings.

Procedural Ruling. Following the Procedural Ruling, the two cases were separated and disputed pure issues of law were identified and determined following Legal Issues Hearings (the ruling on the pure issues of law in IPT/01/77 of 9 December 2004 is considered below). Each claim was then finally determined following the Tribunal's investigation of the cases in closed session. This was similarly the approach taken in *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH).[8]

16. The European Court of Human Rights ("the ECtHR") unanimously upheld the Tribunal's procedural regime as summarised above in *Kennedy v. UK* (2011) 52 EHRR 4, at §§184-191. (*Kennedy* arose out of one of the domestic cases that gave rise to the Procedural Ruling, namely IPT/01/62.)

17. In the Respondents' submission therefore, the approach set out in §~~1414~~ above is the one prescribed in the Rules, is tailored to the subject matter of the matters falling within the Tribunal's jurisdiction, has been expressly accepted as fair and compatible with the ECHR by the ECtHR; and should be followed by the Tribunal in the present Claims.

Formatted: Fo

18. In these proceedings the Claimants seek a public hearing of their complaints (see §10 of Privacy's Grounds and §12 of the Greennet Grounds). It is asserted that documents which have been released into the public domain regarding the alleged technical capabilities and activities of GCHQ mean that there is no good reason to uphold the NCND policy. However, this approach fails to appreciate the ordinary operation of the "neither confirm nor deny" policy in the case of alleged leaks (as set out above). The long-standing general policy is clear: the "neither confirm nor deny" stance is maintained.

19. The Respondents are filing a Closed Response with this Open Response. For the avoidance of doubt, the Respondents' position, with respect to the Tribunal, is that in the light of r. 6 of the Rules, the Procedural Ruling and *Kennedy*, nothing in the Closed Response can be disclosed to the Claimants without the Respondents' consent.

THE RESPONDENT'S OPEN POSITION ON THE FACTUAL ALLEGATIONS

Computer Network Exploitation ('CNE')

20. The allegations made in both claims concern activities known by a number of terms, including "Computer Network Exploitation" or 'CNE'. CNE is a set of techniques through which an individual or organisation gains covert and remote access to equipment (including both networked and mobile computer devices) typically with a view to obtaining information from it.

[8] There is a class of Tribunal cases that have not proceeded in this way (see *e.g. Paton v. Poole Borough Council*, IPT/09/01-05/C, determination of 29 July 2010). But that is because, in these cases, the respondents have decided that the entirety of their factual case can be dealt with in open session, with the result that the Legal Issues Hearing becomes in effect indistinguishable from a substantive hearing on all disputed matters. Where, however, a respondent decides that any part of its factual case is closed, then the approach in §19 applies.

21. CNE operations vary in complexity. At the lower end of the scale, an individual may use someone's login credentials to gain access to information. More complex operations may involve exploiting vulnerabilities in software in order to gain control of devices or networks to remotely extract information, monitor the user of the device or take control of the device or network. These types of operations can be carried out illegally by hackers or criminals. In limited and carefully controlled circumstances, and for legitimate purposes, these types of operations may also be carried out lawfully by certain public authorities.

22. As with interception, there are a range of circumstances in which the Intelligence Services may be required to conduct this type of activity. CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE is used to secure valuable intelligence to enable the State to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

23. CNE operations may enable the Intelligence Services to obtain communications and data of individuals who are engaged in activities which are criminal or harmful to national security in circumstances where it may otherwise be difficult or impossible to so obtain them. Such circumstances may arise where, for example:

    (a) the wanted communications are not in the course of their transmission and cannot therefore be intercepted;

    (b) there is no communications service provider on whom a warrant can be served to acquire particular communications; or

    (c) a more comprehensive set of the target's communications or data of intelligence interest is required than can be obtained through other means.

Response to the specific factual allegations in the Grounds of Complaint

24. In its Grounds of Complaint Privacy International alleges, *inter alia*, that GCHQ is involved in the infection of individuals' computers and mobile devices "*on a widespread scale*"[9] and in a way which "*appears to be indiscriminate in nature*"[10] to gain access either to the functions of the devices (eg. activating a camera or microphone without the user's consent) or to obtain stored data. These allegations are made following alleged disclosures made by the former NSA Contractor Edward Snowden (see §§11-18 of the Privacy Grounds).

25. In their Grounds of Complaint the Greennet Claimants allege, *inter alia*, that GCHQ has targeted internet and service communications providers ('ISPs') in order to compromise and gain unauthorised access to their network infrastructures in pursuit of "*mass surveillance activities*". It is alleged that

[9] See §3 of the Privacy Grounds
[10] See §8 of the Privacy Grounds

there has been manipulation of the ISP's property and unauthorised changes made to its assets and infrastructure, together with surveillance of the ISP's employees and customers respectively (see §55 of the Greennet Grounds). The claims are said to arise out of reports by the German magazine *Der Spiegel* which were also said to arise from alleged disclosures made by Edward Snowden (see §§3-5 and §§13-26 of the Greennet Grounds).

26. The Respondents neither confirm nor deny all of the specific factual claims relating to the alleged specific technical capabilities and/or conduct of GCHQ as set out in the complaints. Further, and for the avoidance of doubt, the Respondents neither confirm nor deny whether there has been any interference with the Claimants' property (whether as alleged in the complaints or otherwise) or that of their employees/clients/customers, and/or whether such interference led to the consideration or examination of any of the Claimants' information or data and/or the information or data of their employees/clients/customers.

27. It is noted that the Claimants make very extreme factual allegations about the scope, scale and nature of GCHQ's activities in these proceedings. For example Privacy asserts that GCHQ's activity "*appears to be indiscriminate in nature*"[11] and that there has been intrusion into "*millions*" of devices which is disproportionate to any legitimate aim[12]. Similarly extreme allegations are also made by the Greennet Claimants, including that GCHQ has engaged in "*mass surveillance activities*"[13]; that its activities are "*indiscriminate*" in nature[14] and amount to "*one of the most intrusive forms of surveillance any government has ever conducted*"[15].

28. No assumption can or should be made as to the truth of <u>any</u> of the Claimants' assertions about the intelligence gathering activities of GCHQ. As noted by the Tribunal in the *Liberty/Privacy* judgment "*the indiscriminate trawling for information...whether mass or bulk or otherwise, would be unlawful, as would be the seeking, obtaining or retention of material which is unnecessary or disproportionate"* (see §160(iii)). Thus, whilst the specific factual allegations which are made in these proceedings are neither confirmed nor denied for the reasons set out above, it is denied that GCHQ is engaged in any unlawful and indiscriminate mass surveillance activities. Such activities are clearly precluded by the clear statutory regime which governs GCHQ's activities as set out in detail below.

29. The Respondents nevertheless accept that the Claimants may challenge the general Art. 8-compatibility of the Equipment Interference Regime on the basis that their property/equipment might <u>in principle</u> have been interfered with and that at least some of their data/information may have been considered or examined.

30. As to Article 10 ECHR, in the light of *Österreichische Vereinigung zur Erhaltung*

[11] §8 of the Privacy Grounds
[12] §51 of the Privacy Grounds
[13] §3 of the Greennet Grounds
[14] §10 of the Greennet Grounds
[15] §61(a) of the Greennet Grounds

v. Austria, Appl. No. 39534/07, 28 November 2013, the Respondents accept that, in the present context, non-governmental organisations (such as Privacy International) engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press. In principle, therefore, any interference with Privacy's communications or communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

31. However the Greennet Claimants cannot claim to be victims of any Art. 10 interferences. They are not journalists, news organisations or a species of NGO which is entitled to claim the protection of Article 10 ECHR (see HMG's skeleton in *Liberty/Privacy* dated 3 July 2014 at §§56-59).

32. Further and in any event Article 10 adds nothing to the analysis under Article 8 ECHR – see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 and see also §12 and §149 of the *Liberty/Privacy* judgment.

33. As to Article 1 of the First Protocol ('A1P1'), this is relied upon by the Greennet Claimants, although it is noted that they advance no evidence in support of the contention that (1) they have suffered any damage or other material alteration of their property, or (2) there has been any damage or detriment to their commercial relationships or loss of goodwill within the meaning discussed in the A1P1 case law (see eg. *R (New London College Ltd) v Secretary of State for the Home Department* [2012] EWCA Civ 51 at §§83-98) (see §37(d) of the Greennet Grounds). This claim therefore appears to be entirely speculative in nature and, in absence of some evidential basis for the alleged interference with their A1P1 rights, including proof of loss and/or damage, should be dismissed. Further and in any event this claim adds nothing to the analysis under Art. 8 ECHR.

THE EQUIPMENT INTERFERENCE REGIME

34. The Equipment Interference Regime which is relevant to the activities of GCHQ principally derives from the following statutes:

    (a) the Intelligence Services Act 1994 ("the ISA"), (as read with the Counter-Terrorism Act 2008 ("the CTA") and the Computer Misuse Act 1990 ("the CMA"));

    (b) the Human Rights Act 1998 ("the HRA");

    (c) the Data Protection Act 1998 ("the DPA"); and

    (d) the Official Secrets Act 1989 ("the OSA").

35. In addition, the draft Equipment Interference Code of Practice dated February 2015 ('the EI Code') is relevant to the regime as regards the scope of any powers to interfere with property and equipment, as are GCHQ's

internal arrangements in relation to CNE activities (see §§99B-99ZS below).

The ISA (read with the CTA and the CMA)

GCHQ functions

36. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

> *"... 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 ...."*

37. By s. 3(2) of the ISA, these functions are only exercisable:

> "*(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*."

38. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... 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 ...*"

Disclosure of information

39. By s. 19(5) of the CTA, information obtained by GCHQ for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*."

40. Thus, specific statutory limits are imposed on the information that GCHQ can obtain, and on the information that it can disclose. In addition, the term "information" is a very broad one, and is capable of covering *e.g.* both communications and communications data.

41. By s. 19(2) of the CTA:

> "*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

Computer Misuse Act ('CMA')

41A. The Computer Misuse Act 1990 (CMA) came into force on 29 June 1990. It was amended on 3 May 2015 as a result of changes introduced by the Serious Crime Act 2015.

42. By s.1(1) of the CMA:

> "*(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*[16] *held in any computer;*
> *(b) the access he intends to secure, is unauthorised*[17]*; and*
> *(c) he knows at the time when he causes the computer to perform the function that that is the case."*

43. Although "*computer*" is not defined in the CMA, in the context of s.69 of the Police and Criminal Evidence Act 1984 (PACE), the term has been held to mean "*a device for storing, processing and retrieving information*" (see *DPP v McKeown* [1997] 1 WLR 295 at 302).

44. By s.3 of the CMA it is also an offence to do any unauthorised act[18] in relation

---

[16] Section 17 of the CMA provides, *inter alia*, that:

> *(2) A person* ***secures access 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 [or to enable such access to be secured] 1) shall be read accordingly.*
> *(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform –*
> *(a) causes the program to be executed; or*
> *(b) is itself a function of the program.*
> *(4) For the purposes of subsection (2)(d) above –*
> *(a) a program is output if the instructions of which it consists are output; and*
> *(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. ...*
>
> *(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.*

[17] By section 17(5) of the CMA – "*Access of any kind by any person to any program or data held in a computer is unauthorised if – (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled"* (NB. this subsection is subject to section 10 which contains a saving in respect of certain law enforcement powers).

[18] By s. 17(8) of the CMA - *An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)– (a) is not himself a person who has responsibility for the computer*

to a computer, if, at the time that he does the act the person knows that it is unauthorised (s. 3(1)) and either (1) the intention is to impair the operation of any computer; to prevent or hinder access to any program or data held in any computer; to impair the operation of any such program or the reliability of any such data (s. 3(2)(a)-(c)), or (2) the person is reckless as to whether the act will do any of those things s. 3(3)).

45. Section 4 of the CMA sets out the territorial scope of, *inter alia*, offences under s. 1 and s. 3 of the CMA. In particular this makes clear that it is immaterial for the purposes of any offence under s.1 or s.3 of the CMA (a) whether any act or other event, proof of which is required for conviction of the offence, occurred in England or Wales; or (b) whether the accused was in England or Wales at the time of any such act or event. Save in respect of certain offences (i.e. under s. 2 of the CMA), at least one significant link with domestic jurisdiction must exist in the circumstances of the case for an offence to be committed. The tests as to whether there is a significant link with domestic jurisdiction are set out in section 5 of the CMA.

46. Summary conviction under the CMA in respect of offences under s. 1 and s. 3 may lead to imprisonment for a term not exceeding 12 months or a fine (see s. 1(3)(a) and s. 3(6)(a) CMA). Any conviction on indictment may lead to imprisonment for a term not exceeding 2 years or to a fine, or both, in respect of a s. 1 offence (see s. 1(3)(c)) and for a term not exceeding 10 years, or to a fine, or both in respect of a s. 3 offence (see s. 3(6)(c) CMA).

46A. Section 10 of the CMA (prior to amendments introduced on 3 May 2015) provided as follows:

> "*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*."

46B. As set out at §37A of the Amended Grounds in the Privacy Complaint, on 3 May 2015 the CMA was amended. Those amendments (which it is accepted are not retrospective) included, *inter alia*:

a) Changes to the test under section 5 as to when a significant link with domestic jurisdiction is established in respect of offences under, *inter alia*, sections 1 and 3 of the CMA;

b) Changes to section 10 of the CMA, which now provides *inter alia*:

> "*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*

---

and is entitled to determine whether the act may be done; and (b) does not have consent to the act from any such person. In this subsection "act" includes a series of acts.

question is authorised or required..."

Authorisation for equipment interference

s.5. warrants

47. By s. 5 of the ISA the Intelligence Services, including GCHQ, can apply for a warrant which provides specific legal authorisation for property interferences by them. Thus by s5(1) of the ISA:

> "*(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.*

48. In relation to GCHQ, pursuant to s.5(2)(a)-(c) of the ISA the Secretary of State can only issue a warrant under s.5 following an application by GCHQ if he/she is satisfied that:

> (a) it is **necessary** for the action to be taken for the purpose of assisting GCHQ in carrying out its statutory functions under s. 3(1)(a) of the ISA;
> (b) the taking of the action is **proportionate** to what the action seeks to achieve; and
> (c) **satisfactory arrangements** are in force under section 4(2)(a) of the ISA with respect to the disclosure of information by GCHQ obtained by virtue of the section and any information obtained under the warrant will be subject to those arrangements.

49. When exercising his/her discretion and considering necessity and proportionality, the Secretary of State must take into account "*whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means*" (s.5(2A) ISA).

50. Pursuant to s. 5(3) of the ISA GCHQ may not be granted a s.5 warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

51. By s.6 of the ISA the procedure for issuing warrants and the duration of s. 5 warrants is addressed. In particular s.6(1) provides that a warrant shall not be issued save under the hand of the Secretary of State, unless it is a species of urgent case as set out in s.6(1)(b) or (d)[19].

52. In terms of duration, unless the warrant is renewed, it ceases to have effect at the end of the period of six months, beginning with the day on which it was

[19] Those sub-sections provide:
(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; ...
(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 any of the specified officials.

issued (s. 6(2)) (save where the warrant was issued urgently and not under the hand of the Secretary of State in which case it lasts for 5 working days).

53. As to renewal, under s.6(3) of the ISA, if, before the expiry of the warrant, the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, it may be renewed for a period of six months.

54. By s. 6(4) of the ISA "*The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary*".

s.7 authorisations

55. In terms only of acts outside the British Islands, s.7 of the ISA also provides for the authorisation of such acts by the Intelligence Services including GCHQ. S.7(1) and 7(2) provide:

> "*(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."*

56. Acts outside the British Islands include cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus (s. 7(9) ISA).[20]

57. However, pursuant to s.7(3) of the ISA, the Secretary of State shall not give an authorisation under s. 7 of the ISA to GCHQ unless he/she 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 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 ...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*

[20] In addition ss.7(10)-(14) of the ISA recognise that it may be difficult, in certain circumstances to ascertain reliably the location of property and therefore provide, *inter alia*, that where acts are done in relation to property which is eg. mistakenly believed to be outside the British Islands, but which is done before the end of the 5th working day on which the presence of the property in the British Isles first becomes known, those acts will be treated as done outside the British Islands.

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

58. Under s. 7(4) of the ISA such an authorisation by the Secretary of State:

"*(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."

59. Consequently the type of acts which may be covered by a s. 7 authorisation are broadly defined in the ISA and can clearly cover equipment interference outside the British Islands, where the tests in s. 7(3) of the ISA are satisfied.

60. By s. 7(5) of the ISA, an authorisation shall not be given except under the hand of the Secretary of State, or in an urgent case and where the Secretary of State has expressly authorised it to be given under the hand of a senior official.

61. In terms of duration, unless it is renewed, a s. 7 authorisation ceases to have effect at the end of the period of six months beginning on the day on which it was given (save if it was not given under the hand of the Secretary of State in which case it lasts for 5 working days) (see s. 7(6) ISA).

62. Pursuant to s. 7(7) the authorisation can be renewed for a period of six months, if the Secretary of State considers it necessary to continue to have effect for the purpose for which it was given.

63. By s. 7(8) of the ISA "*The Secretary of State shall cancel an authorisation if he is satisfied that the action authorised by it is no longer necessary*".

64. Consequently both s. 5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that the Intelligence Services are not civilly or criminally liable for such interferences, including under the CMA.

The draft Equipment Interference Code of Practice dated February 2015 ('the EI Code')

65. The draft Equipment Interference Code of Practice was published on 6 February 2015 by the Home Office. That draft Code was issued pursuant to section 71 of RIPA and is subject to public consultation in accordance with s. 71(3) of RIPA.

66. Whilst the Code is currently in draft, as set out in the Written Ministerial Statement which accompanied its publication, it reflects the current

safeguards applied by the relevant Agencies, including GCHQ. The Agencies will continue to apply with the provisions of the draft Code throughout the consultation period and until the Code is formally brought into force. Consequently GCHQ can confirm that it complies with all aspects of the EI Code and can also confirm that it fully reflects the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by GCHQ.

67. The EI Code provides guidance on the use by the Intelligence Services of s. 5 and s.7 of the ISA to authorise equipment interference to which those sections apply. In particular it provides guidance on the procedures that must be followed before equipment interference can take place, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.

68. To the extent that the EI Code overlaps with the guidance provided in the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014 (see further below), the EI Code takes precedence, however the Intelligence Services must continue to comply with the 2014 Code in all other respects (see §1.2).

69. The EI Code also records the fact that there is a duty on the heads of the Intelligence Services to ensure that *arrangements* are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their statutory functions; and (ii) that no information is disclosed except so far as is necessary for those functions (see §1.3 of the EI Code and the statutory framework under the ISA set out above).

Equipment interference to which the EI Code applies

70. The EI Code identifies specific types of equipment interference to which the code applies. At §1.6 it states:

> "*This code applies to (i) any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:*
>
> *a) obtain information from the equipment in pursuit of intelligence requirements;*
> *b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;*
> *c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);*
> *d) enable and facilitate surveillance activity by means of the equipment.*
>
> *"Information" may include communications content, and communications data as defined in section 21 of the 2000 Act."*

71. At §1.7 of the EI Code it summarises the effect of a s.5 warrant and states:

> "*The section 5 warrant process must be complied with in order properly and effectively to deal with any risk of civil or criminal liability arising from the interferences with equipment specified at sub-paragraphs (a) to (d) of paragraph 1.6 above. A section 5 warrant provides the Intelligence Services with specific legal authorisation removing criminal and civil liability arising from any such interferences.*"

Basis for lawful equipment interference activity

72. In addition to highlighting the statutory functions of each Intelligence Agency, the EI Code specifically draws attention to the HRA and the need to act proportionately so that equipment interference is compatible with ECHR rights. At §§1.10-1.13 the EI Code states:

> "*1.10 The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.*
>
> *1.11 Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the Intelligence Services seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions).*
>
> *1.12 By section 6(1) of the 1998 Act, it is unlawful for a public authority to act in a way which is incompatible with a Convention right. Each of the Intelligence Services is a public authority for this purpose. When undertaking any activity that interferes with ECHR rights, the Intelligence Services must therefore (among other things) act proportionately. Section 5 of the 1994 Act provides a statutory framework under which equipment interference can be authorised and conducted compatibly with ECHR rights.*
>
> *1.13 So far as any information obtained by means of an equipment interference warrant is concerned, the heads of each of the Intelligence Services must also ensure that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of the disclosure of that information, and that any information obtained under the warrant will be subject to those arrangements. Compliance with these arrangements will ensure that the Intelligence Services remain within the law and properly discharge their functions.*"

General rules on warrants

73. Chapter 2 of the EI Code contains a number of general rules on warrants issued under s. 5 of the ISA.

Necessity and proportionality

74. Within Chapter 2 the EI Code contains detailed guidance on the requirements of necessity and proportionality and how these statutory requirements are to be applied in the EI context. At §§2.6-2.8 it states:

> "*2.6 Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.*
>
> *2.7 The following elements of proportionality should therefore be considered:*
>
> - *balancing the size and scope of the proposed interference against what is sought to be achieved;*
> - *explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
> - *considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
> - *evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.*
>
> *2.8 It is important that all those involved in undertaking equipment interference operations under the 1994 Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.*"

75. Consequently the EI Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e. other than the subject of the operation. The EI Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

Collateral intrusion

76. The EI Code also highlights the risks of collateral intrusion involved in equipment interference and provides guidance on how any such issues should be approached, including the need to carry out an assessment of the risk of collateral intrusion. At §§2.9-2.12 it states:

> "*2.9 Any application for a section 5 warrant should also take into account the risk of obtaining private information about persons who are not subjects of the*

equipment interference activity (collateral intrusion).

2.10 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the equipment interference activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

2.11 All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Secretary of State fully to consider the proportionality of the proposed actions."

77. In addition the EI Code makes clear at §2.12 that where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as "*intended intrusion*" and that:

> "*Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above*."

Reviewing warrants

78. At §§2.13-2.15 the Code sets out certain requirements for reviewing warrants and states as follows:

> "*2.13 Regular reviews of all warrants should be undertaken to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years (see Chapter 5). Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.*
>
> *2.14 In each case, unless specified by the Secretary of State, the frequency of reviews should be determined by the member of the Intelligence Services who made the application. This should be as frequently as is considered necessary and practicable.*
>
> *2.15 In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the Intelligence Services should consider whether it is necessary to apply for a fresh section 5 warrant.*"

General best practices

79. The EI Code gives guidance on general best practice to be followed by the Intelligence Services when making applications for warrants covered by the Code. At §2.16 those requirements are:

"• *applications should avoid any repetition of information;*
- *information contained in applications should be limited to that required by the 1994 Act;*
- *where warrants are issued under urgency procedures (see Chapter 4), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application;*
- *where it is foreseen that other agencies will be involved in carrying out the operation, these agencies should be detailed in the application; and*
- *warrants should not generally be sought for activities already authorised following an application by the same or a different public authority."*

80. In addition, the EI Code indicates that it is considered good practice that within each of the Intelligence Services, a designated senior official should be responsible for:

"• *the integrity of the process in place within the Intelligence Service to authorise equipment interference;*
- *compliance with the 1994 Act and this code;*
- *engagement with the Intelligence Services Commissioner when he conducts his inspections; and*
- *where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the Commissioner.*" (see §2.17)

Legally privileged and confidential information

81. Chapter 3 of the Code contains detailed provisions on legally privileged and confidential information which it is intended to obtain or which may have been obtained through equipment interference. In terms of confidential information the Code provides, *inter alia*, at §§3.24-3.27:

"*3.24 Where the intention is to acquire confidential information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to adopting special handling arrangements within the relevant Intelligence Service.*

3.25 Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so in accordance with the statutory functions of each of the Intelligence Services or where otherwise required by law. It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, it must be reviewed at reasonable intervals to confirm that the justification for its retention is still valid

3.26 Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser within the relevant Intelligence Service before any further dissemination of

the material takes place.

3.27 *Any case where confidential information is retained should be reported to the Intelligence Services Commissioner during the Commissioner's next inspection and any material which has been retained should be made available to the Commissioner on request.*"

Procedures for authorising equipment interference under s. 5

82. Chapter 4 of the EI Code sets out the general procedures to be followed for authorising equipment interference activity under s. 5 of the ISA. In that Chapter, §§4.1-4.4 outline the statutory scheme under the ISA. At §4.5 of the code, attention is drawn to the need to consider whether the equipment interference operation might also enable or facilitate a separate covert surveillance operation, in which case a directed or intrusive surveillance authorisation might need to be obtained under Part 2 of RIPA (as addressed in the Covert Surveillance and Property Interference Code).

83. In terms of applications for a s. 5 warrant, the EI Code contains a checklist of the information which each issue or renewal application should contain. At §4.6 it states:

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

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

84. At §4.7-§4.9 of the EI Code the statutory tests for the issuing of a s. 5 warrant

are highlighted, together with the statutory requirements for any urgent authorisation of a s. 5 warrant.

Renewals and cancellations of warrants

85. At §§4.10-4.11 and §§4.12-4.13 of the EI Code the provisions of the ISA addressing the renewals and cancellations of warrants are summarised.

Keeping of records

86. In Chapter 5 of the EI Code provision is made for centrally retrievable records of warrants to be kept for at least three years. At §5.1 it states:

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

- *the date when a warrant is given;*
- *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.*"

Handling of information and safeguards

87. Chapter 6 of the EI Code provides important guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant and makes clear that this information may include communications content and communications data as defined in section 21 of RIPA (§6.1).

88. At §6.2 the EI Code states:

"*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), 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.*"

89. At §§6.6-6.11 of the EI Code key safeguards are set out in the EI Code in terms of the dissemination, copying, storage and destruction of any information obtained as a result of equipment interference. In particular it is stated:

"***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."* (emphasis added)

90. At §§6.4-6.5 the importance of these safeguards is emphasised, together with the need to ensure that each of the Intelligence Services has **internal arrangements** in force for securing that the safeguards are satisfied, which arrangements should be made available to the Intelligence Services Commissioner. In particular it is stated:

"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.*"

Application of the code to equipment interference pursuant to section 7 of the 1994 Act

91. In Chapter 7 of the EI Code it is made clear that "*GCHQ must as a matter of policy apply the provisions of this 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*" (§7.1).

92. Consequently, save as expressly specified in Chapter 7 of the EI Code, all of the provisions of the EI Code, including the important safeguards regarding the processing, retention, disclosure deletion and destruction of any information obtained via equipment interference, apply equally to equipment interference authorised pursuant to s. 7 of the ISA. That is made expressly clear in §7.2 which states:

> "*GCHQ and SIS must apply all the same procedures and safeguards when conducting equipment interference authorised pursuant to section 7 as they do in relation to equipment interference authorised under section 5.*"

93. In addition, Chapter 7 of the EI Code provides specific additional guidance for s. 7 equipment interference authorisations under the ISA.

94. In terms of the general basis for lawful activity under s. 7 of the ISA, the EI Code states at §§7.3-7.6:

> "*7.3 An authorisation under section 7 of the 1994 Act may be sought wherever members of SIS or GCHQ, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located outside the British Islands that would otherwise be unlawful. This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus*[21]*.*
>
> *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).*
>
> *7.5 An application for a section 7 authorisation should usually be made by a member of SIS or GCHQ for the taking of action in relation to that service. Responsibility for issuing authorisations under section 7 rests with the Secretary of State.*
>
> *7.6 An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations. 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 must be sought from a designated senior official (see paragraphs 7.11 to 7.14).*"

95. At §§7.7-7.8 and §§7.9-7.10 the EI Code sets out the statutory tests for s. 7 authorisations, together with the provisions of the statutory scheme dealing with urgent authorisations. At §7.7 the EI Code makes clear that:

> "*Each application should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 equipment interference warrant.*"

[21] However this is "*without prejudice as to arguments regarding the applicability of the ECHR*" as made clear in footnote 17 of the EI Code.

96. Guidance on the types of authorisations under s.7 of the EI Code is also provided at §§7.11-7.14. In particular this provides guidance on any s. 7 authorisations which relate to a broad class of operations. At §§7.11-7.12 it states:

> *"7.11 An authorisation under section 7 may relate to a broad class of operations. Authorisations of this nature are referred to specifically in section 7(4)(a) of the 1994 Act which provides that the Secretary of State may give an authorisation which inter alia relates to "acts of a description specified in the authorisation". The legal threshold for giving such an authorisation is the same as for a specific authorisation.*
>
> *7.12 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 must be sought from a designated senior official. In any case where the equipment interference may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer. Where knowledge of matters subject to legal privilege may be acquired, the Annex A approving officer must apply the tests set out at paragraph 3.4 to 3.7 (and "Secretary of State" should be read as "Annex A approving officer" for these purposes).*

97. For GCHQ an 'Annex A approving officer' means a Director of GCHQ (see Annex A on page 30).

98. In addition §§7.13-7.14 provide guidance on all internal applications for approval, including the need to ensure that such approvals are proportionate and are subject to periodic review at least every 6 months, or more frequently depending on the sensitivity of the operation. Those paragraphs state:

> *"7.13 The application for approval must set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations.*
>
> *7.14 All internal approvals must be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."*

99. As to renewals and cancellations of s. 7 authorisations, the statutory requirements are set out at §§7.15-7.17.

99A. For the avoidance of doubt, and in the light of the clarification requested at

paragraph 47A(b) of Privacy's Amended Grounds, it is the Respondents' position that it is lawful for a s.7 authorisation to relate to a broad class of operations, without a specific and individual "warrant" being made in respect of each individual operation conducted pursuant to that authorisation. As set out above, the EI Code provides for a process of internal approval by a designated senior official to conduct operations under that authorisation.

Internal arrangements

99B. GCHQ also has internal arrangements in relation to s.5 warrants and s.7 authorisations. These are set out below, with gisted passages underlined.[22]

The Compliance Guide

99C. The Compliance Guide is a document which is made available electronically to all GCHQ staff. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

a) Authorised (generally through a warrant or equivalent legal authorisation);

b) Necessary for one of GCHQ's operational purposes; and

c) Proportionate.

99D. These principles, and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

99E. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"*A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ*

[22] The internal arrangements are set out at §§99C to 99ZS. They are added by way of amendment but are not underlined in order to make it clear which passages are gisted.

official of appropriate seniority if a Secretary of State has expressly authorised its use."

Section 5 Guidance

99F. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

99G. The Section 5 Guidance makes clear the nature of the activity which is authorised by a s.5 warrant:

*"**ISA Section 5 guidance***

ISA warrants

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

99H. The geographical, functional and temporal limits of a s.5 warrant are also set out:

*"A **section 5 warrant** authorises interference with property or wireless telegraphy in the British Islands[23]...It may only be issued on grounds of National Security or the Economic Well-Being of the UK. A section 5 warrant is signed by a Secretary of State and is valid for 6 months from the date of signature, at which point the warrant should be renewed or cancelled."*

99I. The guidance mirrors the requirements of s.5(2)(a) and (b) of the ISA. First, it makes clear that the proposed CNE action must be **necessary**:

"Part I. – to be completed by the relevant GCHQ team
The intelligence case should be fit for purpose for signing by a Secretary of State, avoiding unnecessary jargon and technical terminology. The case should include:

- *the intelligence background;*

[23] Both instances of underlining in this quotation are in the original.

- *the priority of the target within the priorities framework as endorsed by JIC[24] and NSC[25];*
- *an explanation of why the proposed operation is necessary;*
- *a description of any other agency involvement in working the target;*
- *the intelligence outcome(s) the proposed operation is expected to produce."*

99J. The requirement that the proposed CNE action be **proportionate** is also made clear:

"As CNE techniques are by nature intrusive, an explanation of how proportionality will be maintained should be given. Key points to consider include:
- *the expected degree of invasion of a target's privacy and whether any personal or private information will be obtained;*
- *the likelihood of collateral intrusion, ie invading the privacy of those who are not targets of the operation, eg family members;*
- *whether the level of intrusion is proportionate to the expected intelligence benefit;*
- *a description of the measures to be taken to ensure proportionality."*

99K. The Section 5 Guidance stipulates that each request for a warrant, or warrant renewal, must have a sponsor of an appropriately senior level:

*"**Requesting a new Section 5***
Requests for new warrants and renewals must be sponsored by an appropriately senior official, who must be satisfied that the proposed operation is justified, proportionate and necessary."

99L. The Section 5 Guidance requires that, once completed, the warrant request must be returned to its "sponsor" for consideration of whether it passes the test set out in s.5(2)(a) and (b) of the ISA, before being signed and sent to the relevant personnel:

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

99M. The Section 5 Guidance also explains that the process is completed by the preparation of a formal submission and a warrant instrument. These are reviewed by GCHQ Legal Advisers and the sponsor, then sent for signature to the relevant Department, which will follow its own internal procedures before the documents are passed to the Secretary of State for consideration. Once the warrant has been signed, relevant personnel will be informed that the operation can go ahead.

99N. A designated form must be filled out when a section 5 warrant is sought. The specified information reflects the requirements of the guidance on section 5 warrants, and includes the following:

[24] Joint Intelligence Committee.
[25] National Security Council.

a) Under "Intelligence Case"

"why is CNE necessary and why can the expected intelligence not be gained by other less intrusive means[26]?"

"what intelligence the operation is expected to deliver

b) Under "Degree of intrusion, including collateral intrusion"

"how far will the operation intrude on the privacy of the target? Is the operation likely to obtain personal or private information?

to what extent will the operation affect those not of operational interest (eg could the individual's computer be used by family members, friends or colleagues who are not targets of the operation)?

how will the intelligence gained justify the expected level of intrusion?

what measures will be put in place to ensure proportionality is maintained."

(c) Under "Recipients of Product":

"where within GCHQ is the product of the CNE operation to be sent?"

(d) Finally, the Request must be authorised by the appropriately senior GCHQ official, who must, inter alia, certify that "*The proposed CNE operation is justified, proportionate and necessary*".

Renewals of s.5 warrants

99O. The Section 5 Guidance also details the procedure for renewals of section 5 warrants. This requires specific attention to be paid, *inter alia*, to whether the operation is still justified, necessary and proportionate at the time of the renewal:

"***Section 5 renewal process***
A reasonable period before a warrant is due to expire, the relevant personnel will request a case for renewal from the relevant personnel, copying the sponsor and include a copy of the previous submission. The analyst should confirm with the sponsor that renewal is required, and if so, provide the relevant personnel with a business case by the specified deadline. This should include:

- *an update of the intelligence background, ensuring it accurately reflects the current context of the warrant;*
- *details of any developments and intelligence gained since the warrant was issued/last renewed – this **must** address any expectations highlighted in the previous submissions;*
- *a review of the level of intrusion, based on the evidence of the activity authorised by the warrant;*
- *a review and, if necessary, update of the political aspects of the risk assessment;*

[26] Underlining in the original.

The relevant team should provide the following information:

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

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

Cancellation of s.5 warrants

99P. The Section 5 Guidance also addresses cancellation of warrants, making clear that as soon as warrants are no longer required they should be cancelled:

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

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

Section 5 cancellation process
When a warrant is no longer required, the analyst should send the relevant personnel a short explanation of the reason for the cancellation. When the team conducting the operation confirms that the operation is fully drawn down, the relevant personnel will draft a letter based on this feedback and submit it, with a cancellation instrument, to the issuing Department for signature (usually by a senior official rather than the Secretary of State)."

Section 7 Guidance

99Q. GCHQ's guidance which governs applying for, renewing and cancelling section 7 authorisations/internal approvals is set out both in the Compliance Guide (in the section dealing with authorisations) and in separate internal guidance ("the Section 7 Guidance"). The process set out in the Section 7 Guidance has been subject to the scrutiny and advice of the Intelligence Services Commissioner who has confirmed that he is content with the process.[27]

[27] In addition to the Intelligence Services Commissioner's suggestions in his June 2013 inspection, and his approval of GCHQ's consequent changes in his December 2013 inspection, during a visit in December 2014 GCHQ presented to and discussed with the Intelligence Services Commissioner, the "end to end" process regarding CNE operations using two operational case-studies. The class-authorisation, internal approvals and additions authorisations were considered. The Commissioner was then shown how CNE operators conduct the operations with a live demonstration of an operation. There was also a focus on the relevant forms (which were discussed in some detail). The Commissioner indicated that he was content with the format and the level of detail in the forms.

99R. The Section 7 Guidance requires any CNE activities overseas to be carried out pursuant to a s.7 authorisation in order for such activities to be lawful under domestic law. Authorisations may either be specific to a particular operation or to a broad class of operation:

*"**ISA Section 7 guidance***

ISA authorisations

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

99S. The Section 7 Guidance sets out the 'class authorisations' signed by the Secretary of State under section 7 of the ISA which are used by GCHQ for the majority of its active internet-related operations. In respect of the authorisations relevant to CNE the Section 7 Guidance states that it:

"*permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant). The interference includes CNE operations."*

99T. The Section 7 Guidance also stipulates that such authorisations need to be renewed every six months, and assert the vital importance of providing information to the Secretary of State to justify any renewal:

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

99U. The requirement, in addition to a section 7 class authorisation, for a section 7 approval for a specific operation, and the procedure for obtaining such an approval, is set out both in the section of the Compliance Guide on CNE, and also in the Section 7 Guidance. The latter emphasises, *inter alia*, the importance of considering and setting out, in a request for a section 7 approval, why an operation against a target is necessary and proportionate, and the requirement that a copy of the signed approval be sent to the FCO:

*"**ISA section 7 internal approvals***

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

99V. The Section 7 Guidance explains the importance of this process, including the provision of signed approvals to the FCO, for ensuring that operations are necessary, justified and proportionate is again stressed:

"This process provides the necessary reassurance to FCO that operations carried out under the class authorisations are necessary, justified and proportionate."

99W. Necessity (including why means other than a CNE operation could not be used) and proportionality (particularly with regard to the privacy of a target or any third party) are addressed in more detail under *"Section B – business case/necessity/proportionality":*

"The business case should…include:

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

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

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

99X. The Section 7 Guidance makes clear, under "Completing the process" that the internal approval will then be provided to an appropriately senior GCHQ official for signature and for, *inter alia*, the setting of a review period for the internal approval:

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

99Y. The standard form used for seeking section 7 approvals reflects both the Section 7 Guidance and the statutory criteria. In particular it sets out the following:

a) *"**Business case, including***
- *Intelligence background (to include brief details of what has been achieved from other accesses).*
- *What you expect to get from using CNE techniques against this target set & how the intelligence gained will justify the expected level of intrusion.*
- *Any timing factors or special sensitivities.*

…"

b) *"**Necessity, including***
- *The necessity of conducting CNE operations against this target set (an explanation of why the use of CNE techniques is necessary)."*

c) ***"Proportionality and consideration of intrusion into privacy, including***
- *The proportionality of conducting CNE operations against this target set (CNE operations are intrusive by nature, and are likely to obtain information which is personal and private). Confirm that you have assessed that the level of intrusion into privacy, including collateral intrusion, is justified and proportionate. Outline measures to be put in place to ensure proportionality is maintained."*

The term "*privacy"* is defined *"in the broadest sense to mean a state in which one is not observed or disturbed by others".*

99Z. The appropriately senior GCHQ official who must support any request for a section 7 approval has to certify, *inter alia*, that:

"Operations conducted under this approval are justified, proportionate and necessary."

99ZA. The relevant form also makes clear that the request for an approval should be sent to the relevant personnel at request stage, review stage and cancellation stage. Where an addition to an approval is sought the relevant personnel must also be consulted.[28] As a matter of practice, and as required by the Section 7 Guidance, final versions of s.7 approvals are sent to the Foreign and Commonwealth Office. A monthly summary report which summarises new s.7 approvals, reviews of s.7 approvals and cancellations, and also attaches copies of new approvals, is also sent to the relevant senior official at the FCO.

99ZB. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an "addition" to an existing approval is required.

99ZC. The "additions form" requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

[28] A reference to "relevant personnel" is to staff who are responsible for securing legal/policy approvals, checking the relevant risk assessments and maintaining compliance records.

Review of s.7 internal approvals

99ZD. Approvals must be reviewed, and upon each review consideration is required to be given to whether the operation is still necessary and proportionate, specifically having regard to issues of intrusion and privacy. The process of reviewing s.7 approvals is summarised in the Section 7 Guidance as follows:

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

99ZE. The review and revalidation is held at intervals determined by the designated GCHQ senior official who originally signed the section 7 approval. These are more frequent for particularly sensitive operations. The Section 7 Guidance also sets out a procedure for recording the history of a section 7 approval from the original submission through to any review or cancellation:

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

99ZF. Thus the approval process, including any review, is recorded so that the history of and basis (including necessity and proportionality) for any approval, review or cancellation, is available for audit.

Cancellation of s.7 internal approvals

99ZG. The Section 7 Guidance also stipulates the need to cancel internal approvals as soon as an operation is no longer needed:

> *"**Cancelling a section 7 internal approval***
> *To show due diligence and as a condition of relying on the class authorisations, section 7 internal approvals should be cancelled when an operation is no longer needed. To help ensure that this happens, the relevant personnel will ask whether section 7 internal approvals are still needed as part of the class authorisation renewals process, and if so will seek a brief rejustification of the continuing necessity and*

proportionality. The number of approvals signed or cancelled is provided to the Foreign Secretary with the case for renewal.

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

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

99ZH. The Section 7 Guidance therefore contains safeguards against section 7 approvals remaining in place where they are no longer necessary and/or proportionate.

Obtaining data

99ZI. There are further safeguards in place to ensure that decisions by CNE operators to obtain data from implanted devices are lawful. In particular:

a) In addition to a formal process of training and examination which all CNE Operators have to undergo, all CNE operators must every two years also undertake advanced legalities training which is specific to active operations such as CNE (in addition to the basic legalities training which all staff are required to complete).

b) CNE operators can obtain legal advice at any time.

c) In addition, any data obtained in an operation will be available to the relevant intelligence analysts for that project, who in turn will be aware of the legal authorisation for the project, and will also have completed legalities training. The CNE section of the Compliance Guide provides guidance for intelligence for intelligence analysts requesting a particular document to be retrieved.

99ZJ. Thus, the obtaining of data is subject to the same requirements of necessity and proportionality as the initial process of obtaining an authorisation/warrant/approval.

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 be 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.

99ZO. 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.

Training

99ZS. In addition to the training referred to at paragraphs 99ZI(a) and 99ZR above, GCHQ does provide some training for analysts on particular CNE activities, which reiterates the substance of the Section 7 Guidance. GCHQ is currently in the process of revising the training referred to at paragraph 99ZI(c) to incorporate more detail on CNE.

Oversight by the Intelligence Services Commissioner

100. In §§8.1-8.2 of the EI Code the important role of the Intelligence Services Commissioner in the use of the powers under the ISA is emphasised. In particular §8.2 states:

> "*It is the duty of any member of the Intelligence Services who uses these powers to comply with any request made by the Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions. Such persons must also report any action that is believed to be contrary to the provisions of the 1994 Act to the Commissioner.*"

The Covert Surveillance and Property Interference Code ('the Property Code")

101. The Covert Surveillance and Property Interference Code ("the Property Code") provides guidance on entry on and interference with property by public authorities under s. 5 of the ISA (see the Code at §1.2) and applied to activity including equipment interference. That Code was also issued pursuant to s. 71 of RIPA which stipulates that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in, *inter alia*, s.5 of the 1994 Act. The Property Code was first issued in 2002 and further versions of the Code were published in 2010 and on 10 December 2014 (in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code).

102. As set out above, to the extent that there is an overlap between the EI Code and the Property Code, the EI Code takes precedence in terms of equipment interference under s. 5 of the ISA. In those circumstances the Respondents have set out below only a brief overview of the key provisions of the Property Code.

(a) Chapter 3 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA and in particular guidance is given as to the requirement of proportionality and the factors to be taking into account when making a proportionality assessment.
(b) The question of collateral intrusion is also directly addressed in §§3.8ff of the Code.
(c) As to the procedures to be followed for reviewing authorisations, the Code provides for regular reviews of all property interference authorisations (see §§3.23-3.25).
(d) The Code also highlights best working practices which are to be followed by all public authorities with regard to all activities covered

by the Code (see §§3.28-3.29).

(e) Chapter 4 of the Code contains special provisions on legally privileged and confidential information.

(f) Chapter 7 of the Code contains authorisation procedures for property interference. This specifically addresses authorisations for property interferences by the Intelligence Services at §§7.36-7.38.

(g) Chapter 8 of the Code provides that certain records shall be kept of property interferences which are authorised which are to be centrally retrievable for three years (see in particular §8.3).

(h) In Chapter 9 of the Code guidance is given as to the handling of material obtained through property interference. §9.3 of the Code addresses the retention and destruction of material and states as follows:

> "*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 ... property interference...*"

(i) In addition the Code states at §9.7 that, in relation to the Intelligence Services:

> "*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 ... 1994 Act.*"

(j) Finally Chapter 10 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

> "*The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ.*"

The HRA

103. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

> "*(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.*"

104. Art. 10 of the ECHR, which is similarly a Convention right (and which is similarly set out in Sch. 1 to the HRA), provides:

> "*(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema*

enterprises.
(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

105. By s. 6(1):

"*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

106. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, GCHQ must (among other things) act proportionately and in accordance with law. In terms of equipment interference activity, the HRA applies at every stage of the process i.e. from authorisation, through to the obtaining, retention, handling and any disclosure/dissemination of such material.

107. S. 7(1) of the HRA provides in relevant part:

"*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –*
(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."

The DPA

108. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data (as defined in s. 1(1) of the DPA) that it holds. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

109. Consequently as a data controller, GCHQ is in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services (including GCHQ) are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services (including GCHQ) from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5. Personal data processed*[29] *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."[30]

110. Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged:

(a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

(b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

111. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of GCHQ that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

112. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Oversight mechanisms

113. There are three principal oversight mechanisms in respect of the equipment interference regime:

(a) The Intelligence Services Commissioner

---

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

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

(b) The ISC; and

(c) The Tribunal.

The Intelligence Services Commissioner

114. As highlighted in the relevant Code, the Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within the ISA by the Intelligence Services including GCHQ.

115. The Prime Minister is under a duty to appoint a Commissioner (see s. 59(1) of RIPA). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.

116. Under s. 59(7) of RIPA, the Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 59(2), which provides in relevant part:

> *"…the [Commissioner] shall keep under review, so far as they are not required to be kept under review by the Interception of Communications Commissioner-*
> *(a) the exercise by the Secretary of State of his powers under sections 5 to 7 of... the Intelligence Services Act 1994..."*

117. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.

118. In practice, the Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Representative samples of warrantry paperwork are scrutinised, including the paperwork for s. 5 and/or s.7 ISA warrants/authorisations. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Commissioner also meets with the relevant Secretaries of State.

119. S. 60 of RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)

120. The Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed

openly.

121. S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.

122. In addition, the Commissioner is required by s. 59(3) to give the Tribunal:

> "*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
> *(a) in connection with the investigation of any matter by the Tribunal; or*
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter*."

123. The Tribunal is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

124. The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the equipment interference regime, see §8.3 of the Code.

125. It is to be noted that in the *Liberty/Privacy* judgment the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

The ISC

126. GCHQ is responsible to the Foreign Secretary,[31] who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

127. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA").

128. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.

129. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a

[31] The Director of GCHQ must make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State (see s. 4(4) of the ISA).

member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

~~130. The current chair is Sir Malcolm Rifkind MP. He is a former Secretary of State for Defence and a former Secretary of State for Foreign and Commonwealth Affairs.~~

131. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.

132. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

133. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

134. It is to be noted that in the *Liberty/Privacy* judgment, the Tribunal placed considerable emphasis on the important oversight which is provided by the ISC (see in particular §44 and §121 of the judgment); the Tribunal describing the ISC as "*robustly independent*" at §121.

The Tribunal

135. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

136. The Tribunal's jurisdiction is broad. As regards the Equipment Interference regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:

(a) The Tribunal has exclusive jurisdiction to consider claims under s.

7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

(b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) of RIPA).

137. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).

138. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, interfered with or disclosed information emanating from interferences with property/equipment in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged obtaining, interference with or disclosure of information.

139. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.[32] As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

140. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §138~~138~~ above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

Formatted: Fo

141. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.

142. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

[32] The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish *e.g.* that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

ISSUE OF PURE LAW SUITABLE FOR DETERMINATION AT A LEGAL ISSUES HEARING

143. It is submitted that the following issue of pure law can be identified from the Grounds advanced by the Claimants:

Issue: Does the Equipment Interference Regime satisfy the "in accordance with the law" requirement in Art. 8(2)?

144. The remaining grounds of claim do not give rise to pure issues of law which are suitable for determination at a Legal Issues Hearing. Rather, these grounds of claim turn on factual assertions that are neither confirmed nor denied, and which are relevant to the determination of the "proportionality" issues raised. It follows that they must - as necessary - be investigated and considered by the Tribunal in closed session in the light of such relevant closed evidence, if any, as is filed by the Respondents. The Respondents invite the Tribunal to investigate these grounds of claim in closed session after holding a Legal Issues Hearing.

145. As set out earlier in this Response, Article 10 adds nothing to the analysis under Article 8 ECHR – see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 and see also §12 and §149 of the *Liberty/Privacy* judgment and therefore this has not been addressed separately below. In addition the A1P1 complaint on the part of the Greennet Claimants (1) is wholly unsupported by any evidence of loss and/or damage to its property or possessions and (2) adds nothing to the analysis under Art. 8 ECHR. In those circumstances this has also not been addressed separately below.

Issue: Does the Equipment Interference Regime satisfy the requirements in Art. 8(2) that any interference be "in accordance with the law"

The test to be applied

146. The expression "in accordance with the law" requires:

> "*... firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law ...*" (*Weber*, at §84.)

Domestic law

146A. It is denied that any carrying out of CNE operations by GCHQ pursuant to warrants/authorisations issued under s.5 and s.7 of the ISA, prior to the coming into force of the Serious Crime Act 2015 (which amended the CMA), was not in accordance with domestic law, whether as alleged in §37 and §41B(a) of Privacy's Amended Grounds, or at all. Without prejudice to the generality of that denial, the Respondents' position can be summarised as follows:

a) In enacting the ISA in 1994, after the coming into force of the CMA in

1990, Parliament made specific provision for the Intelligence Services, including GCHQ, to conduct activities which might otherwise be unlawful (whether under criminal or civil law), where the activity was authorised by s. 5 warrants or s. 7 authorisations. That is clear from the express language of the ISA and, in particular at s.5(1) and s.7(1)-(2), as set out at §47 and §55 above.

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

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

d) S.10 of the CMA (prior to being amended on 3 May 2015) did not have the effect that only lesser interferences, amounting to a breach of s.1 of the CMA, could be authorised, including under the ISA or RIPA, as alleged in §37 and §41B(a) of Privacy's Amended Grounds. That section was directed at "certain law enforcement powers" (see the title to s. 10) i.e. powers of inspection, search or seizure (eg. by the police) and it did not purport to set out the circumstances in which, what would otherwise be offences under the CMA, might be authorised eg. by the Intelligence Services when exercising their statutory functions including in the interests of national security and the prevention and detection of serious crime.

e) The amendments to s.10 CMA were clarificatory only, as is evident from the explanatory notes to that section, set out at §37C of Privacy's Amended Grounds and as made clear in the Home Office Fact Sheet to the Serious Crime Act 2015 (Part 2: Computer Misuse) and the Home Office Circular, both dated March 2015, which stated as follows:

> "*Section 44 clarifies the savings provision at section 10 of the 1990 Act and is intended to remove any ambiguity for the lawful use of powers to investigate crime (for example under Part 3 of the Police Act 1997) and the interaction of those powers with the offences in the 1990 Act. The changes do not extend law enforcement agencies' powers but merely clarify the use of existing powers (derived from other enactments, wherever exercised) in the context of the offences in the 1990 Act*." (Home Office Fact Sheet)
>
> "*Section 44 clarifies section 10 of the CMA. Section 10 of the CMA*

contained a saving provision whereby criminal investigations by law enforcement agencies did not fall foul of the offences in the Act. However, section 10 pre-dates a number of the powers, warrantry and oversight arrangements on which law enforcement now rely to conduct investigations, such as those in Part 3 of the Police Act 1997. The changes do not extend law enforcement agencies' powers but merely clarify the use of the existing powers (derived from other enactments, wherever exercised) in the context of the offences in the CMA." (Home Office Circular)

f) The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect unless there was an express savings provision in each relevant piece of legislation (whether governing criminal or civil liability), making clear that it was without prejudice to powers set out in any other enactment. That is manifestly inconsistent with the scheme of the ISA. It also elevates the status of savings provisions eg. in the CMA, beyond that which is tenable. As has been recognised in the case law, savings provisions are a frequently unreliable guide to the provisions to which they attach, since savings provisions "*are often included by way of reassurance, for the avoidance of doubt or for an abundance of caution*"[33].

146B. In the premises the submissions at §37 and §41B(a) of Privacy's Amended Grounds are wrong in law and misconceived.

146C. As to §§37D, 37F, 41B(b) and 47A of Privacy's Amended Grounds:

a) The Respondents confirm that, as a matter of practice, any CNE activities carried out abroad, or over a foreign computer, even if the relevant user is located in the United Kingdom, would be authorised by an authorisation issued under section 7 ISA.

b) The very purpose of section 7 of the ISA is to provide for the granting of authorisations in respect of any act done outside the British Islands, where otherwise a person would be liable under the criminal or civil law of the UK. In addition, section 7(9) of the ISA makes clear that such authorisations can relate to an act which is done in the British Islands, but which is or is intended to be done in relation to apparatus that is believed to be outside the British Islands.

c) In those circumstances any questions as to the applicability and/or effect of section 31 of the Criminal Justice Act 1948 ('the CJA') are irrelevant in these proceedings.

d) Without prejudice to that, the Respondents do not accept that section 31 of the CJA extends the scope of the territorial jurisdiction provisions in the CMA (see §37F of Privacy's Amended Grounds), nor

[33] See Lord Simon of Glaisdale in *Ealing London Borough Council v Race Relations Board* [1972] AC 342 at 363.

are the broad assertions in §41B(b) of Privacy's Amended Grounds accepted as an accurate statement of the law. In particular:

i) It is denied that the offences under the CMA are capable of being transposed under the CJA, in circumstances were the CMA makes clear what significant link with domestic jurisdiction is necessary in order for any offence to be committed. If a significant link with jurisdiction is not, in fact, present, it is denied that an offence will have been committed, whether under the CMA or the CJA.

ii) Further and/or alternatively and without prejudice to sub-paragraph (i) above, even if the CJA did apply, the question whether there was any liability under section 31 of the CJA, read with the CMA, would depend upon the specific circumstances in question including, *inter alia*, the answers to the following key questions:

(1) Whether the offence was contrary to the laws of the foreign country i.e. it would only be where the Crown Servant commits an offence contrary to the laws of the foreign country and which would be indictable in England, that section 31 of the CJA could apply; and

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

146D. As to paragraph 41C of Privacy's Amended Grounds:

1. The references to sections 5 and 7 ISA 1994 are noted.
2. Insofar as necessary, the interpretation of the said provisions will be the subject of submission in due course.
3. The meaning of the terms "thematic" and "class" as used by Privacy are not understood in this context. Neither term forms part of the statutory requirements for the issue of a warrant under section 5.
    a. If and insofar as the term "thematic" used by Privacy refers to the usage by the Intelligence Services Commissioner in his 2014 Report at page 18, the following matters are noted:
        i. As set out at paragraph 47 above, section 5(1) provides: "No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section." That provision does not delimit the scope of a warrant to any single piece of property or single instance or method of entry on to or interference with property or wireless telegraphy.

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

iii. Whether action and/or any property and/or wireless telegraphy is "specified" in a warrant will depend upon the words used in the particular warrant.

iv. If and to the extent that it is the Claimant's case that the terms "any property so specified" in section 5(2) are to be read as precluding the Secretary of State from issuing a warrant save in relation to a particular operation against a particular piece of property, that is denied.

v. For the avoidance of doubt, "property" can be "specified" in a section 5 warrant by description. Such description may encompass more than one particular location or item of property.

b. The term "class" is not used by Commissioner in his Report in connection with section 5 warrants. It is a term used by him in connection with section 7 authorisations.

4. It is denied that warrants issued (and acts authorising warrants) under section 5 ISA 1994 were or are unlawful. It is averred that the Secretary of State can only sign a warrant if satisfied that the activity thereby authorised is necessary and proportionate.

146E. Paragraph 41D of Privacy's Amended Grounds is denied. Insofar as necessary, the interpretation of sections 5 and 7 ISA 1994 (and the significance or otherwise of the wording of ss.5(3) and (3A)) will be the subject of submission in due course.

146F. To the extent that paragraph 41E of Privacy's Amended Grounds is understood it is denied:

a. The nature or type of the alleged interference with copyright is unduly vague and inadequately pleaded (by reference to other allegations made or otherwise).

b. Further, the relevance of Directive 2001/29 is not understood. The relevant law of copyright is the domestic law of England and Wales and no breach thereof is alleged. It is not contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law. For the avoidance of doubt, it is noted that Directive 2001/29 was implemented in the United Kingdom in particular in the Copyright Designs and Patents Act 1988 (as amended).

c. Further or alternatively, insofar as it is relevant, it is denied that (i) the actions of the Defendant pursuant to the protection of national

security interfere with any rights protected under Directive 2001/29; and/or (ii) any interference with such rights by the actions of the Defendants is unlawful or disproportionate.

146G. Paragraph 41F of Privacy's Amended Grounds and its relevance is denied. Submissions on the nature, terms and effect of the judgment in Case C-293/12 will be made as necessary in due course. For the avoidance of doubt, the said judgment, inter alia, was not concerned with copyright, did not consider standards required for derogations under Directive 2001/29 (the relevance of which is not understood – see paragraph 146F(b) above) and did not purport to lay down "the standard required to justify a derogation from EU law rights" whether in relation to "surveillance" or otherwise.

Articles 8 and 10 ECHR

147. In relation to 'foreseeability' in this context, the essential test, as recognised in §68 of *Malone v. UK* (1984) 7 EHRR 14 and in §37 and §118 of the *Liberty/Privacy* judgment, is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*". As the Grand Chamber recently confirmed in the eavesdropping case of *Bykov v. Russia*, appl. no. 4378/02, judgment of 21 January 2009, this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §78 , as quoted at §37 of the *Liberty/Privacy* judgment).[34]

148. Consequently the key question when considering whether the Equipment Interference Regime satisfies the "in accordance with the law" test under Art. 8(2) is whether there are:

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

149. As noted by the Tribunal in the *Liberty/Privacy* judgment, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §38-40 and §137). That was made very clear by the Strasbourg Court at §§67-68 of *Malone* and in *Leander v Sweden* [1987] 9 EHRR 433 at §51 and *Esbester v UK* [1994] 18 EHRR CD 72, as quoted at §§38-39 of the Tribunal's judgment in *Liberty/Privacy*.

[34]The "necessity" requirement also calls for adequate and effective safeguards against abuse. But the Tribunal is sufficient for this purpose: §59 of *Rotaru v. Romania* (2000) 8 BHRC 449 ("*effective supervision ... should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure* ..."). *A fortiori*, the combination of the Tribunal, the ISC and the Commissioner satisfies this aspect of the "necessity" requirement.

150. Thus, as held by the Tribunal in the *British Irish Rights Watch* case dated 9 December 2004 (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87):

> "*foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...*" (§38)

151. Consequently the national security context and the particular national security justification for the activity/conduct which is impugned is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment).

152. Moreover, the ECtHR has consistently recognised that the foreseeability requirement "*cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly*": *Malone v. UK* (1984) 7 EHRR14, at §67; *Leander v. Sweden* at §51; and *Weber*, at §93.

153. As to the procedures and safeguards which are applied, two important points should be noted.

154. First it is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* and in *Bykov* at §78 and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*.

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

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

156. Although these conclusions were reached in the context of the s. 8(4) RIPA interception regime, they are equally applicable to the equipment regime where the relevant IE Code and Property Code both refer expressly to undisclosed statutory "arrangements" under the ISA (see eg. §1.3 of the IE Code and §7.38 and §9.7 of the Property Code) and where there is similar oversight by the Intelligence Services Commissioner.

157. In terms of oversight mechanisms, it is important to note the extent to which the Tribunal in *Liberty/Privacy* placed reliance on these mechanisms when concluding that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8(2) complaint. Thus the Tribunal highlighted the advantages of the Tribunal as an oversight mechanism at §46 and the importance of these oversight mechanisms in the s. 8(4) regime at §122. Therefore, as the ECtHR recognised in §95 of *Weber*, account should be taken of all the relevant circumstances, including:

> "*the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, judgment of 28 June 2007, at §77.)

Application to the Equipment Interference Regime

158. In terms of the criticisms which are made of the legal framework in the Claimants' Grounds, the Respondents make the following six points in this response and pending further clarification of the Claimants' case in due course.

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

160. The ECtHR has expressly referred to the fact that "rather strict standards" apply in the interception context, but do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* (2011) 53 EHRR 24, at §66 and *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, *per* Lord Carswell at §85. There is no factual or legal justification for asserting that an even stricter set of standards ought to apply to equipment interference activities, over and above those which would apply eg. to an interception case.

161. **Secondly**, contrary to the assertion made in the Grounds, there is a clear legal framework governing any equipment interference activities, as set out in detail earlier in this Response. The availability of warrants under s. 5 and authorisations under s. 7 of the ISA, do provide a firm legal framework which is supplemented in important respects by the CMA, HRA, the DPA, the OSA, the EI Code, GCHQ's internal arrangements and the Property Code. That statutory scheme, in common with the interception regime in RIPA, makes

certain activities an offence (as is the case eg. in s. 1 of RIPA which makes it an offence, without lawful authority to intercept certain communications) but is coupled with a regime for the issuing of warrants/authorisations which render the activity lawful if strict conditions are satisfied. The suggestion that the availability of a warrant under the ISA "*simply cancels any unlawfulness*" is a misrepresentation and an over-simplification of the statutory scheme and the safeguards which are inherent within it.

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

163. **Thirdly** it is wrong to suggest that there is no Code of Practice governing equipment interference. As has been set out in detail above, there has always been a Code which governed property interference (including equipment interference) and there is now a bespoke Code, the EI Code, which contains important safeguards including, *inter alia*:

(a) Detailed guidance on the requirement of proportionality and the considerations which apply in the equipment interference context, including issues such as collateral intrusion and the need to consider less intrusive alternatives (Chapter 2);
(b) Guidance on the frequency of reviews, particularly where there is a high level of intrusion into private life or significant collateral intrusion or confidential information is likely to be obtained (Chapter 2 at §§2.13-2.15);
(c) Best practice guidance on applications for warrants/authorisations (§§2.16-2.17);
(d) Special considerations which should apply to legally privileged and confidential information (Chapter 3);
(e) Detailed and comprehensive procedures for the authorisation of both s. 5 and s. 7 ISA equipment interference activity (see Chapters 4 and 7);
(f) Important record keeping requirements in respect of any equipment interference (Chapter 5);
(g) Comprehensive safeguards and guidance as regards the processing, retention, disclosure, deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant, which mirror similar safeguards applied as part of the interception regime pursuant to s. 15 of RIPA (Chapter 6)..

<u>In addition, GCHQ's internal arrangements contain safeguards as set out at §§99B-99ZS above.</u>

164. **Fourthly** it is submitted that the Equipment Interference Regime does indicate the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (*Malone*, at §68). In overview:

(a) The regime is sufficiently clear as regards the circumstances in which there can be interferences with equipment. Any warrants/authorisations in respect of equipment interference by the Intelligence Services can only be issued if clear statutory criteria are satisfied, including the requirements of necessity and proportionality and such permission can only be given by the Secretary of State personally, save in an urgent case.

(b) The regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of any information so obtained. In this regard the ISA must be read in conjunction with other important safeguards in the CTA, the DPA, the HRA, the OSA and the Codes.

165. Further, if some version of the list of "safeguards" in *e.g.* §95 of *Weber* applies to the Equipment Interference Regime, the present regime satisfies the requirements for such "safeguards", insofar as it is feasible to do so.

(a) The first and second requirements in *Weber* i.e. the "offences" which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read , in particular, with §1.6, §§4.1-4.4 and §7.8 of the IE Code. It is also to be noted that the term "*national security*" is a sufficient description in the ISA (see §116 of the L*iberty/Privacy* judgment).

(b) The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 2, 4, 6 and 7 of the IE Code and GCHQ's internal arrangements. In particular:

(a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled. In addition the IE Code contains important provisions on reviewing warrants and the frequency of reviews (see §2.13-2.15).

(b) There are detailed safeguards which apply which mirror the safeguards in s.15 of RIPA in the interception regime, as regards the handling, dissemination, copying, storage, destruction and security arrangements for information obtained as a result of equipment interference (see in particular Chapter 6 of the IE Code). Further GCHQ must ensure that there are internal arrangements in force, which are approved by the Secretary of State, for securing that the requirements set out in Chapter 6 of the IE Code are satisfied in relation to all information obtained by equipment interference (see §6.4 of the IE Code) and these internal arrangements should be made available to the Commissioner (see §6.5 of the IE Code).

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

(d) In addition any disclosure of such information must satisfy the constraints imposed in s. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA;

(e) There is also the requirement for statutory arrangements to be in place, by reference, in particular, to the ISA (s. 4(2)(a) and the EI Code itself makes reference to such arrangements at §1.3;

(f) Any disclosure eg. deliberately in breach of the "arrangements" for which provision is made in s.4(2)(a) of the ISA would be criminal under s.1(1) of the OSA.

166. **Fifthly** the Tribunal can take into account the "*below the waterline*" rules, requirements and arrangements which regulate any equipment interference activities which may be conducted by GCHQ. These have been addressed above (at §§99B-99ZS) and separately in GCHQ's Closed Response to the complaints. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime.

167. **Finally** there are important oversight mechanisms which are relevant to the Article 8(2) compatibility of the regime including the Tribunal, the ISC and the Intelligence Services Commissioner. These oversight mechanisms are centrally relevant to the question whether the regime provides for adequate protection against abuse. The combination of these oversight mechanisms is a very important safeguard in the context of the Art 8(2) compatibility of the regime.

168. In conclusion the Equipment Interference Regime is sufficiently accessible and "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2).

169. In relation to paragraph 52A of Privacy's Amended Grounds paragraphs 146F-G above are repeated.

~~SUGGESTED DIRECTIONS~~

~~170. The Respondents invite the Tribunal to make the following directions, prior to any directions hearing:~~

~~(a) Within 21 days of service of this Response, the Claimants shall confirm in writing whether the Issues for the Legal Issues Hearing~~

~~that are identified in this Response are agreed and, to the extent that they are not, shall set out the pure issues of law which they propose should be determined at that hearing. The Claimants to be at liberty to file Replies by the same date.~~

~~(b) Within 21 days thereafter the parties to file and serve their suggested directions for the management of the Claims up to and including the Legal Issues Hearing.~~

~~171. The Respondents would be content for the Tribunal to hold a public *inter partes* directions hearing to determine the procedure to be adopted in the two Claims. They respectfully submit that any directions hearing be listed on a date when all counsel are able to attend, given the specialist nature of the proceedings. At any directions hearing, the Respondents will propose that the two Claims be formally joined.~~

6 February 2015
28 May 2015
25 September 2015
13 November 2015

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