IN THE INVESTIGATORY POWERS TRIBUNAL
(THE PRESIDENT AND THE VICE-PRESIDENT)

09 DECEMBER 2004

IN THE MATTER OF APPLICATION NO IPT/01/77

# RULINGS OF THE TRIBUNAL ON PRELIMINARY ISSUE OF LAW

Counsel for the Complainants: Mr Richard Clayton QC and Mr Gordon Nardell instructed by Mona Arshi, Liberty.

Counsel for the Respondents: Mr Philip Sales and Mr Ben Hooper instructed by Treasury Solicitor.

1. The various complaints and claims by the Complainants have been dealt with together by the Tribunal. They include allegations of interference with privacy by accessing telephone and other communications. The Tribunal has not addressed the substance or truth of any such allegations at this stage and has not heard any evidence. This hearing was to deal with a number of preliminary issues of law requiring resolution in the claims, at the same time as preliminary issues relating to the parallel claim by the Complainant in Application No IPT/01/62.

2. The Respondents to the claims are the Security Service, GCHQ and the Secret Intelligence Service. As a result of a considerable amount of work by the Complainants and the Respondents, including compliance with orders of the Tribunal for the articulation and, so far as possible, agreement of any possible outstanding such preliminary issues, the dispute between the parties was considerably narrowed down; and in the event by the conclusion of the hearing only one issue has required to be addressed.

3. The issue was whether, as formulated by the Complainants' Counsel, "*the process of filtering intercepted telephone calls made from the UK to overseas telephones ... breaches Article 8(2)* [of the European Convention on Human Rights] *because it is not 'in accordance with the law'*". Article 8 reads 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 prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

4. Although prior to and during the hearing the Complainants had formulated, and sought to pursue, claims for relief against the Respondents arising out of such conclusions as this Tribunal might reach, if favourable to the Complainants, by further written submissions dated 2 August 2004 any such claims were no longer pursued. Thus the issue for the determination of the Tribunal is simply the lawfulness of the "*filtering process*", relating to material obtained pursuant to a warrant issued under s8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA").

5. RIPA provides for two different "regimes": the s8(1) regime with regard to the interception of communications transmitted and received within the United Kingdom ("internal telecommunications") and the s8(4) regime, relating to telephone communications between the United Kingdom and abroad ("external communications"). However, there are, as will be seen, substantial similarities between the provisions governing such regimes. In particular, both the s8(1) and s8(4) warrants are subject to the provisions of s5 of RIPA, which provides for the issue of warrants in relation to the interception of communications by the Secretary of State in subsection (1).

6. The relevant provisions governing both regimes are contained in the following subsections of s5:

> "*(2) The Secretary of State shall not issue an interception warrant unless he believes –*
>
> *(a) that the warrant is necessary on grounds falling within subsection (3); and*
>
> *(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.*
>
> *(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary –*
>
> *(a) in the interests of national security;*
>
> *(b) for the purpose of preventing or detecting serious crime;*
>
> *(c) for the purpose of safeguarding the economic well-being of the United Kingdom; or*
>
> *(d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.*
>
> *(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.*
>
> ...
>
> *(6) The conduct authorised by an interception warrant shall be taken to include –*
>
> *(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;*
>
> *(b) conduct for obtaining related communications data; and*
>
> *(c) conduct by any person which is conduct in pursuant of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect of the warrant.*"

7. So far as the warrants themselves are concerned, the domestic, or s8(1) warrant, is far more circumscribed in its effect than an external or s8(4) warrant, because it can only be issued for the purpose of interception of communications relating to one identified person ("*the interception subject*") or a single set of premises: see subsection 8(1) of RIPA. There must, by s8(2), be a schedule or schedules to the warrants "*setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted*", directed towards or identifying the *interception subject* or the relevant *single set of premises* (subsection 8(3).

8. None of this specificity of individual subject or premises applies to an s8(4) warrant relating to external communications, which is governed by the two following subsections:

> "*(4) Subsections (1) and (2) shall not apply to an interception warrant if –*
>
> *(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and*
>
> *(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying –*
>
> *(i) the descriptions of intercepted material the examination of which he considers necessary; and*
>
> *(ii) that he considers the examination of material of those descriptions necessary as mentioned in s5(3)(a), (b) or (c).*
>
> *(5) Conduct falls within this subsection if it consists in -*
>
> *(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and*
>
> *(b) any conduct authorised in relation to any such interception by s5(6).*"

9. The s8(4) warrant is accordingly also described as a "*certificated warrant*". It can and may result, provided that the requirements of s8(4) and (5) are satisfied, in the interception of all communications between the United Kingdom and an identified city or country.

10. Counsel for the Complainants put forward no challenge to the lawfulness of a s8(1) warrant, either as to the procedure by which interception is ordered and the intercepted material obtained, nor with regard to the procedures by which decisions are made as to the "*accessing*" of such material once so intercepted, i.e. decisions as to which parts or which conversations, out of a mass of material obtained pursuant to a s8(1) warrant, will be listened to and/or recorded. Nor do the Complainants raise any challenge to the lawfulness

of a s8(4) warrant itself or to the interception of material pursuant to such warrant. The challenge is limited, as set out in paragraph 4 above, to the lawfulness of the *filtering* process of what is obtained under a s8(4) warrant and as to the absence of, or absence of publicity of, "*selection criteria*" as to what is to be accessed in relation to material obtained pursuant to a s8(4) warrant.

11. It is apparent that the interference with the privacy of communications is likely to be greater by virtue of a s8(4) warrant than as a result of what Counsel called a "*targeted*" s8(1) warrant; although there may still be a mass of material obtained pursuant to a s8(1) warrant, dependent upon the activities of the individual, or at the premises, the subject of the warrant, and the number of calls made. In relation to both regimes, there are restrictions upon the use of intercepted material. S15 in particular applies to both a s8(1) and a s8(4) warrant. By s15(1) the Secretary of State must ensure in relation to all interception warrants that such arrangements are in force as he considers necessary for securing, by reference to s15(2), that there is the minimum necessary disclosure and copying of such material, and by reference to s15(3) the soonest possible destruction. No challenge is any longer made by the Complainants to the processes relating to disclosure, retention or destruction of material obtained under a s8(1) or a s8(4) warrant. There are extra safeguards provided by s16 of RIPA in the case of s8(4), or *certificated*, warrants. S16 reads in material part as follows:

> "*(1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a s8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it –*
>
> > *(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and*
> >
> > *(b) falls within subsection (2).*
>
> *(2) Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which –*
>
> > *(a) is referable to an individual who is known to be for the time being in the British Islands; and*
> >
> > *(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.*

12. There are then provisions in subsections (3) to (5) which allow exceptions to this limitation.

13. Finally, within certain limited exceptions provided in s18, disclosure of the contents of an intercepted communication in court proceedings is prevented.

14. As to the safeguards in ss15 and 16 of RIPA, in his witness statement served on behalf of the Respondents, the Director General of the Organised Crime, Drugs and International Group of the Home Office explains as follows:

> "*26. The internal agency manuals that set out the section 15 and section 16 safeguards, contain comprehensive instructions and refer in detail to specific techniques and processes. This level of detail is required precisely in order to ensure that the section 15 and section 16 safeguards, and the section 8(4) requirements, are properly understood by staff and are fully effective in practice. For the reason given in the above paragraph* [his description of the growing threat of terrorism, and the use by terrorist groups of modern technology, requiring to be countered by interception techniques and appropriate levels of secrecy to protect those techniques] *the Government is unable to disclose the full detail of the arrangements for s8(4) warrants that are in place under sections 15 and 16 of* [RIPA]. *Disclosure of the specific arrangements, the Government assesses, and I believe, would be contrary to the interests of national security. In particular, it would enable individuals to adapt their conduct so as to undermine the operational effectiveness of any interception efforts which it might be thought necessary to apply to them. It is axiomatic that such instructions would be a very great utility to, for instance, members of the intelligence agencies of countries that are hostile to British interests.*
>
> *27. In the light of the above, what I set out in this statement is the fullest account of the safeguards and operating procedures that the Government is able to provide without undermining national security. The Government has experience of the loss of intelligence available to it and the loss of effectiveness of its intelligence gathering machinery, consequent upon revealing details of the methodologies available to it.*"

15. As we have indicated, it is only with regard to the *filtering process*, or the disclosure of *selection criteria*, as to the accessing of material obtained, and only in relation to a s8(4) warrant, that Counsel's submissions have been directed. The Complainants relied, however, upon a statement from an experienced expert, who is a writer and technical telecommunications consultant (among others to the Science and Technology Options Assessment office of the European Parliament), albeit one prepared when the Complainants' critique was directed considerably more widely. The relevant criticism which the Complainants now draw from that statement was summarised, by reference to that statement, by the Complainants' Counsel:

> "*17.1 that the search terms and filtering criteria for filtering are <u>not</u> specified in the* [Secretary of State's] *certificates* ...
>
> *17.2 that search terms and filtering criteria are selected and administered by civil servants without reference to the judiciary or ministers* ...

*17.3 that search terms and filtering criteria can be changed at will ...*

*17.4 that no material describing the filtering process has been published.*"

16. The Complainants rely in this regard on what is described as the materially different treatment of s8(1) and s8(4) warrants by the Interception of Communications Code of Practice issued pursuant to s71 of RIPA ("the Code of Practice"). Subparagraph 4.2 of the Code of Practice deals with the application for a s8(1) warrant as follows:

> "*An application for a warrant is made to the Secretary of State. ...Each application, a copy of which must be retained by the applicant, should contain the following information:*
>
> - *Background to the operation in question*
> - *Person or premises to which the application relates (and how the person or premises feature in the operation).*
> - *Description of the communications to be intercepted, details of communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.*
> - *Description of the conduct to be authorised as considered necessary in order to carry out the interception, where appropriate.*
> - *An explanation of why the interception is considered to be necessary under the provisions of section 5(3).*
> - *A consideration of why the conduct is to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.*
> - *A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.*
> - *Where an application is urgent, supporting justification should be provided.*
> - *An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of the Act.*

17. Applications for a s8(4) warrant are addressed in subparagraph 5.2 of the Code of Practice:

> "*An application for a warrant is made to the Secretary of State ...each application, a copy of which must be retained by the applicant, should contain the following information:*
>
> - *Background to the operation in question* [identical to the first bullet point in 4.2].
> - *Description of the communications ... [this is materially identical to the third bullet point in 4.2].*
> - *Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to*

*intercept those external communications, where appropriate [compare the wording of the fourth bullet in 4.2].*

- *The certificate that will regulate examination of intercepted material.*
- *An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes* [identical to the fifth bullet point in 4.2].
- *A consideration of why the conduct should be authorised by the warrant is proportionate* ... [identical to the sixth bullet point in 4.2].
- *A consideration of any unusual degree of collateral intrusion* ... [identical to the seventh bullet point in 4.2].
- *Where an application is urgent* ... [identical to the eighth bullet point in 4.2].
- *An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2) - 16(6) of the Act.*
- *An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of the Act* [these last two bullets of course are the equivalent to the last bullet point in 4.2].

18. By subparagraph 4.8, the s8(1) warrant instrument should include "*the name or description of the interception subject or of the set of premises in relation to which the interception is to take place*" and by subparagraph 4.9 there is reference to the schedules required by s8(2) of RIPA. The equivalent provision in relation to the format of the s8(4) warrant in subparagraph 5.9 does not of course identify a particular interception subject or premises, but requires inclusion in the warrant of a "*description of the communications to be intercepted*".

19. The Complainants' Counsel points out that, whereas for a s8(1) warrant it is necessary, and presumably therefore practicable, for there to be prior identification of an individual and/or a set of premises, such is not required for a s8(4) warrant, nor specified by the provisions of the consequent Code of Practice provision. It is submitted that it ought to be practicable and, it seemed to be suggested, necessary, for a similar identification of individuals whose communications are to be accessed pursuant to a s8(4) warrant before they are accessed, or at least identification or publication of criteria by which such individuals are to be selected. It is submitted that this identifies a difference between a s8(1) regime and s8(4) regime, which renders the one lawful and the other unlawful.

20. It is, however, entirely clear to us that insofar as the Complainants' submissions depend upon the finding of such a distinction between the two regimes, this cannot be supported:

20.1 The basis of the two warrants is obviously different. This is because it is the more necessary for additional care to be taken with regard to interference with privacy by

a Government in relation to domestic telecommunications, with regard to which it has substantial potential control; but also because its knowledge of, and certainly its control over, external communications is likely to be dramatically less. As a result, the domestic regime, so far as permitted interception is concerned, is considerably tighter. However, although there is that difference, it is a difference relating to what material is permitted to be *intercepted* as a result of a warrant and, as set out in paragraph 10 above, no challenge is made to the lawfulness of either warrant so far as the lawfulness of the interception is concerned.

20.2 Given the differences in the warrant, the difference in the provisions of the Code of Practice is both natural and justified. It is only a s8(1) warrant which requires the identification or description of a particular person or premises, because it is to that person or premises alone to which the interception is to attach. As is necessary under the very provisions of RIPA itself, both warrants require justification by reference to s5(3) as to the grounds/necessity for interception, and both require consideration, by reference to s5(2)(b) and (4), of proportionality.

20.3 It is clear to us that once the material is intercepted under the two different warrants, there is in fact no difference in treatment with regard to *accessing* that material, albeit that the quantity of material obtained under a s8(4) warrant may be greater or more diverse than that obtained under a s8(1) warrant – though that is not necessarily the case, depending upon the frequency of communication. The Respondents' Counsel submitted that, as a matter of common sense, once the material has been intercepted and before it has been listened to, those about to access will not know what they are going to hear, will not know how many conversations, and between whom, have been recorded, and indeed, even on listening to the conversations, may not have any idea to whom they are listening. Even more so in relation to material obtained pursuant to a s8(4) warrant it is unlikely that they would have any idea of what individuals or what premises are involved. It is therefore not comparing like with like for the Complainants' Counsel to suggest that there could or should be some kind of similar consideration prior to accessing s8(4) material, so far as identification of possible individuals or premises are concerned, to that required to be gone through prior to the application for a s8(1) warrant.

21. The Complainants' Counsel at least as characterised by the Respondent's Counsel, was submitting that there should or could be some criteria formulated for the benefit of an individual whose communication might be accessed as part of the material intercepted under a s8(4) warrant, so as to assist him in understanding "why me?" He accepted that, even in relation to the preparation for a s8(1) warrant, where identification of an individual or at least premises is required in the warrant, it would not be feasible for criteria to be formulated, or certainly published, in relation to such identification. It is clear that it would be even less feasible for there to be any kind of formulation, not to speak of publication, of criteria with regard to the identification of those who may, or may not, turn out to be recorded in a mass of material, not yet listened to, which has been lawfully intercepted pursuant even to a s8(1) warrant, not to speak of a s8(4) warrant.

22. It appeared to us that there was a lack of clarity in the Complainants' argument in this regard. Far from there being a distinction between a s8(1) warrant and a s8(4) warrant at the access stage, the treatment is identical. It is at the proposed interception stage that there must be identification of individuals for a s8(1) warrant; but at the access stage (i.e. once the material has been obtained), the position under both warrants so far as access is concerned is identical. There either are no selection criteria or certainly are none published with regard to either warrant; and the Complainants' Counsel makes (and rightly so in our judgment) no complaint about their absence with regard to the access stage in relation to a s8(1) warrant. It is perhaps significant that when the Complainants' Counsel first formulated his proposition in relation to s8(4) warrants, he complained of the "*absence of any publicly stated material indicating that a relevant person is satisfied that the interception of a particular individual's telephone call is proportionate*". On its face of course that is right, because of the very difference between the two warrants, but such is not in fact the complaint. The complaint is as to the absence of published criteria for filtering the intercepted material for the purposes of *accessing* (and the Complainants' submission was so amended). In that regard, however, there are, as we have discussed, no criteria published in relation to either warrant. If anything, it would seem that, as is to be expected, there is additional protection in relation to a s8(4) warrant, because of the additional provision in s8(4)(b)(ii) whereby, at the time of the issue of the warrant, the Secretary of State must certify that he considers the examination of the material to be intercepted from the communications, as described in the warrant, to be necessary for the purposes specified in s5(3)(a), (b) or (c).

23. We are satisfied that, insofar as the Complainants' submissions are based upon an alleged differential between the treatment of s8(1) and s8(4) warrants, they cannot be supported.

24. It is, as the Complainants rightly submit, for the Respondents to establish that the accessing of information obtained pursuant to a s8(4) warrant, falls within the exception of "*in accordance with law*" as set out in Article 8(2). The jurisprudence is now well settled in this regard, that there are three requirements of the "*in accordance with law*" element:

(i) The interference must have some basis in domestic law.

(ii) It must be adequately accessible; and

(iii) It must be formulated so that it is sufficiently foreseeable.

25. There is no challenge to the establishment of the first requirement. The Complainants' challenge relates to *accessibility* and *foreseeability*. Reliance is placed on Lord Clyde's statement in **DeFreitas v Minister of Agriculture** [1999] 1 AC 69 at 78E-F, that it is the concept of legal certainty which underpins these requirements and upon the decision in **Silver v United Kingdom** [1983] 5 EHRR 347, in which the European Court of Human Rights, applying the earlier decision of **Sunday Times v United Kingdom** [1979] 2 EHRR 245, concluded that the United Kingdom had failed to act *in accordance with law* in relying, in relation to the administration of prisons, on standing orders and instructions which were unpublished at the relevant time. It is submitted that when officials access material intercepted under a s8(4) warrant, and do so without any published selection criteria, they are not doing so *in accordance with law*. Reliance is placed primarily upon the decision of the European Court of Human Rights in **Valenzuela Contreras v Spain** [1998] 28 EHRR 483, particularly at 503, where the Court sets out in paragraph 46, that:

> "*The following principles relevant in the instant case have been established by the Court in its case law*:
>
> *(i) The interception of telephone conversations constitutes an interference by a public authority in the right to respect for private life and correspondence. Such an interference will be in breach of Article 8(2) unless it is "in accordance with the law", pursues one or more legitimate aims under paragraph 2, and, in addition, is "necessary in a democratic society" to achieve those aims.*
>
> *(ii) The words "in accordance with the law" require first that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law, but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law*

*against arbitrary interference by public authorities with the rights safeguarded by paragraph 1. From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him.*

*(iii) Especially, where a power of the executive is exercised in secret, the risks of arbitrariness are evident. In the context of secret measures of surveillance or interception by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated.*

*(iv) The* ***Kruslin*** [[1990] 12 EHRR 528] *and* ***Huvig*** [[1990] 12 EHRR 547] *judgments mention the following minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people likely to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and the circumstances in which the recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court."*

26. In the course of his submissions, the Complainants' Counsel made clear that he did not rely on the suggestion that the "*definition of the categories of the people likely to have their telephone tapped*" should be "*set out in the statute*". He submitted that it was possible, and in this case necessary, to supplement the material in the statute through the Code of Practice, and that this Code of Practice is deficient in that regard. At one stage he sought to draw some distinction between telephone calls originated in the United Kingdom and those originated abroad, but he did not pursue such suggestion, and it is obviously impracticable.

27. The Complainants' Counsel referred to the words of Lord Slynn in **R (Alconbury) v Secretary of State for Environment** [2003] AC 295 at para 26, whereby he stated:

> "*In the absence of some special circumstances, it seems to me that the court should follow any clear and constant jurisprudence of the European Court of Human Rights. If it does not do so there is at least a possibility that the case will go to that court, which is likely in the ordinary case to follow its own constant jurisprudence.*"

28. Although later in his submissions Complainants' Counsel put his case on the basis that there was no doctrine of binding precedent in the European Court of Human Rights, nevertheless he himself had not only drawn our attention to the words of Lord Slynn but

also to those of Lord Bingham in **R (Anderson) v Secretary of State for the Home Department** [2003] 1 AC 837 at 879 para 18:

> "*While the duty of the House under section 2(1)(a) of the Human Rights Act 1998 is to take into account any judgment of the European Court, whose judgments are not strictly binding, the House will not without good reason depart from the principles laid down in a carefully considered judgment of the court sitting as a Grand Chamber.*"

29. We are satisfied that the passages in the judgment of the Court in **Valenzuela Contreras** do not in fact articulate or set out support for Complainants' proposition, at least without full consideration of their context, and that in any event what Counsel seeks to derive from it is not the "*clear and constant jurisprudence of the European Court of Human Rights*".

29.1 As is quite clear from the way in which the principles are formulated, both **Valenzuela Contreras** itself, and indeed **Kruslin** and **Huvig,** to which reference is made, were cases in the context of the making of a judicial order leading to the purported admissibility of evidence obtained by telephone tapping in a subsequent criminal trial: and in any event it is in the context of a targeted order, equivalent to a s8(1) warrant, which explains the reference to the requirement, for which Counsel does not contend, for the naming in a statute of "*people liable to have their telephones tapped by judicial order*".

29.2 A very significant aspect to the passage in the European Court's judgment, which is only apparent from the footnotes to it, which are incorporated in the judgment, is the express approval of the Court's earlier decision in **Malone v United Kingdom** [1984] 7 EHRR 14. There is by virtue of such footnotes an express cross-reference to **Malone** with regard to the penultimate sentence of subparagraph (ii) of the passage, namely to paragraph 67 of the Court's judgment in that case, and again in relation to the passage in the second sentence of subparagraph (iii), where the Court is referring to what the requirement of foreseeability implies, namely the giving to citizens of "*an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures*". The relevant passage in paragraph 67 in **Malone** which is being cross-referred to, and plainly approved, by the Court reads:

> *"Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly."*

This must be a fortiori where it is not the *purpose of preventing or detecting serious crime* which is at stake but *the interests of national security*. The Complainants' Counsel fully accepts, and himself drew our attention to, such cases as **Klass v Germany** [1978] 2 EHHR 214, in which the Court recognised the fact that "*democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction*" (para 48 at 232].

29.3 Reliance upon **Valenzuela Contreras** must also be tempered by subsequent jurisprudence, to which we now turn.

30. The Respondents' Counsel placed considerable reliance upon the decision of the Commission in **Christie v United Kingdom** [1993] 78-ADR 119. This decision took express account of, and referred to, **Kruslin** and **Huvig** (at 132). It was considering the very legislation now before us (save that it related to the predecessor statute, the Interception of Communications Act 1985, the terms of s2(2) of which were materially identical to s5(3) of RIPA). It was not a question of a judicial order for evidence leading to its admissibility in court. The issue related to authorised interception of telexes received from trade unions in Eastern Europe, which had been considered necessary under s2(2) (now s5(3)). Accessibility and foreseeability were addressed, and there was express reference not only to the **Sunday Times** judgment but also to paragraph 67 of the **Malone** judgment. The Commission concluded at 133ff as follows:

> *"The Government contend that the terms of the relevant legislative provisions sufficiently indicate the type of activity likely to be susceptible to interception of communications, and that safeguards are imposed that regulate the retention and use of information obtained from interceptions.*
>
> *The Commission notes that the case law of the Commission and Court establishes that the requirement of foreseeability in the special context of sectors affecting*

*national security cannot be the same as in many other fields. In the* ***Leander*** *case* [[1987] 9 EHRR 433] *the Court stated:*

> *"Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally ... the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life ..."*

*The Commission recalls that it has considered the compatibility with the requirements of foreseeability of the partial definition of "interests of national security" ... in two previous cases,* ***Esbester v United Kingdom*** [[1994] 18 EHRR CD 72]*...and* ***Hewitt and Harman v United Kingdom*** [Commission decision 1.9.93]*... It considered that the principles referred to above did not necessarily require a comprehensive definition of the notion of "the interests of national security", noting that many laws, which by their subject matter require to be flexible, are inevitably couched in terms which are to a greater or lesser extent vague and whose interpretation and application are questions of practice. It held that, given the express limitations on the exercise of the Security Service's functions and the supervision of a Tribunal and Commissioner, the law was formulated with sufficient precision ...*

*While, as the applicant points out, the provisions of the 1985 ...* [Act] *are not subject to the influence of the adversarial input which forms part of the judicial process of interpretation, the Commission does not consider that the concept of foreseeability requires that questions of interpretation and practice must be decided in a judicial forum. It is compatible with the requirements of foreseeability that terms which are on their face general and unlimited are explained by administrative or executive statements and instructions, since it is the provision of sufficiently precise guidance to enable individuals to regulate their conduct, rather than the source of that guidance, which is of relevance (cf ...* ***Silver*** *...). ...*

*In light of the above, the Commission considers that the scope and manner of exercise of the powers to intercept communications and make use of the information obtained are indicated with a requisite degree of certainty to satisfy the minimum requirements referred to above.*

*The Commission thus concludes that any interference in the present case was "in accordance with the law".*"

31. The Complainants' Counsel submits that **Christie** and the two previous decisions referred to can be distinguished, since, although the issue addressed related to the identical statutory provision, the precise point now being taken was not addressed, namely one directed towards the absence of selection criteria. As will be seen however, it is the Respondents' submission that s5(3) supplies the answer to the Complainants' new submission also, such that, if that be right, the submission is both not new and answered by **Christie**.

32. The nub of the Complainants' contention is that this is a case which falls within **Silver**, because there is no answer provided by the statute, and no other guidelines, published or available, which supply an answer to the requirement of accessibility or foreseeability:

32.1 Although the Complainants' expert referred to a case presented to the Constitutional Court in the Federal Republic of Germany, in which there was reference made to a list of search terms which could or might be used as a filtering system prior to accessing material (although, as the Respondents' Counsel points out, he does not himself appear actually to say that the German search terms were ever published, as opposed to an account being given to the German Constitutional Court), the Complainants' Counsel does not suggest that, in order to comply with the *in accordance with law* doctrine there would have to be publication in the United Kingdom of a list of search terms. Such a course would in our judgment be both risky and pointless; risky because it would or might, contrary to the principle enunciated in paragraph 67 of **Malone**, enable those intending to participate in secret communications to avoid the use of words which would be known to appear in the search list; and pointless both for that reason and because any accessing of information intercepted pursuant to a s8(4) warrant would be bound to be fact-specific, and what was being looked for would depend upon the subject matter of the warrant.

32.2 At the end of the day the Complainants' Counsel's submission is a simple one. He is in no position, he submits, to guess at what should be said, but he simply submits that something more should be said, by way of indication as to selection criteria than is presently stated, and that the selection should not be left simply to the discretion of officials.

33. The Respondents' response is unequivocal. They refer to paragraph 22 of the statement mentioned above in paragraph 14:

> "... *This process under section 8(4) permits selection and examination of the selected material only to the extent that to do so would be necessary in the interests of national security, to prevent or detect serious crime or to safeguard the economic well-being of the United Kingdom. In this regard and generally, section 8(4) is to be read in conjunction with section 15 of* [RIPA], *which in subsection (1)(b) specifically makes section 8(4) warrants subject to arrangements for ensuring that the requirements of section 16 of* [RIPA] *are satisfied (namely "that intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary as mentioned in section*

*5(3)(a), (b) or (c)"). It is the duty of the Secretary of State to ensure that such arrangements are in force that he considers necessary for securing that the requirements of s16 are satisfied."*

34. The selection criteria in relation to accessing a large quantity of as yet unexamined material obtained pursuant to a s8(4) warrant (as indeed in relation to material obtained in relation to a s8(1) warrant) are those set out in s5(3). The Complainants' Counsel complains that there is no "*publicly stated material indicating that a relevant person is satisfied that the* [accessing] *of a particular individual's telephone call is proportionate*". But the Respondents submit that there is indeed such publicly stated material, namely the provisions of s6(1) of the Human Rights Act which requires a public authority to act compatibly with Convention rights, and thus, it is submitted, imposes a duty to act proportionately in applying to the material the s5(3) criteria.

35. To that duty there is added the existence of seven safeguards listed by the Respondents' Counsel, namely (1) the criminal prohibition on unlawful interception (2) the involvement of the Secretary of State (3) the guiding role of the Joint Intelligence Committee ("JIC") (4) the Code of Practice (5) the oversight by the Interception of Communication Commissioner (whose powers are set out in Part IV of the Act) (6) the availability of proceedings before this Tribunal and (7) the oversight by the Intelligence and Security Committee, an all-party body of nine Parliamentarians created by the Intelligence Services Act 1994, whose operation is described in the Respondents' evidence. The existence of the Commissioner and the Tribunal alone expressly weighed with the Commission in its decision in **Christie**.

36. It is plain that, although in fact the existence of all these safeguards is publicly known, it is not part of the requirements for accessibility or foreseeability that the precise details of those safeguards should be published. The Complainants' Counsel has pointed out that it appears from the Respondents' evidence that there are in existence additional operating procedures, as would be expected given the requirements that there be the extra safeguards required by s16 of the Act, and the obligation of the Secretary of State to ensure their existence under s15(1)(b). It is not suggested and by the Complainants that the nature of those operating procedures be disclosed, but that their existence, i.e. something along the lines of what is in the Respondents' evidence, should itself be disclosed in the Code of Practice.

37. We are unpersuaded by this. First, such a statement in the Code of Practice, namely as to the existence of such procedures, would in fact take the matter no further than it already

stands by virtue of the words of the statute. But in any event, the existence of such procedures is only one of the substantial number of safeguards which are known to exist. Accessibility and foreseeability are satisfied by the knowledge of the criteria and the knowledge of the existence of those multiple safeguards.

38. It is in those circumstances that the Respondents submit, by reference to the criteria in s5(3), as exercised with proportionality and the existence of the multiple safeguards, that both the question and the answer are the same as in **Christie**. We agree. It is clear from the **Sunday Times** case at para 49 that foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security, as discussed in **Klass** and **Leander**. This is not a **Silver** case where the legislation itself was inadequate and the guidelines were unpublished. In this case the legislation is adequate and the guidelines are clear. Foreseeability does not require that a person who telephones abroad knows that his conversation is going to be intercepted because of the existence of a valid s8(4) warrant. The "why me?" test is as inapt in this case as it would have been found to be by the Court of Appeal in its recent decision in **R ex parte Gillan and Another v Commissioner of Police for the Metropolis** [2004] 3 WLR 1144, at paragraph 50 of the judgment of the Court given by Lord Woolf LCJ, in relation to the subject of a valid stop and search order.

39. The provisions, in this case the right to intercept and access material covered by a s8(4) warrant, and the criteria by reference to which it is exercised, are in our judgment sufficiently accessible and foreseeable to be *in accordance with law*. The parameters in which the discretion to conduct interception is carried on, by reference to s5(3) and subject to the safeguards referred to, are plain from the face of the statute. In this difficult and perilous area of national security, taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed upon the Respondent, we are satisfied that the balance is properly struck.