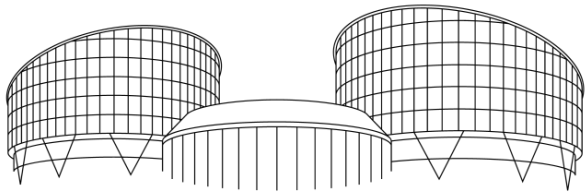

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF KENNEDY v. THE UNITED KINGDOM

(Application no. 26839/05)

JUDGMENT

STRASBOURG

18 May 2010

FINAL

18/08/2010

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Kennedy v. the United Kingdom**,**

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Lech Garlicki, *President*,
Nicolas Bratza,
Giovanni Bonello,
Ljiljana Mijović,
Päivi Hirvelä,
Ledi Bianku,
Nebojša Vučinić, *judges*,
and Lawrence Early, *Section Registrar*,

Having deliberated in private on 27 April 2010,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 26839/05) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a British national, Mr Malcolm Kennedy ("the applicant"), on 12 July 2005.

2. The applicant was represented by N. Mole of the AIRE Centre, a non-governmental organisation based in London. The United Kingdom Government ("the Government") were represented by their Agent, Ms E. Willmott of the Foreign and Commonwealth Office.

3. The applicant complained about an alleged interception of his communications, claiming a violation of Article 8. He further alleged that the hearing before the Investigatory Powers Tribunal was not attended by adequate safeguards as required under Article 6 and, under Article 13, that he had as a result been denied an effective remedy.

4. On 14 November 2008 the Vice-President of the Fourth Section decided to give notice of the application to the Government. It was also decided to examine the merits of the application at the same time as its admissibility (Article 29 § 3).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. Background facts

5. On 23 December 1990, the applicant was arrested for drunkenness and taken to Hammersmith Police Station. He was held overnight in a cell shared by another detainee, Patrick Quinn. The next day, Mr Quinn was found dead with severe injuries. The applicant was charged with his murder. The applicant alleged that the police had framed him for the murder in order to cover up their own wrongdoing. In September 1991, the applicant was found guilty of the murder of Mr Quinn and was sentenced to life imprisonment. In February 1993, his conviction was overturned on appeal. At a first retrial, one of the police officers, a key prosecution witness, failed to appear. He was subsequently declared mentally unstable and was withdrawn from the proceedings. Following a second retrial, the applicant was convicted in 1994 of manslaughter and sentenced to nine years' imprisonment. The case was controversial in the United Kingdom on account of missing and conflicting police evidence which led some – including a number of Members of Parliament – to question the safety of the applicant's conviction.

6. In 1996, the applicant was released from prison. Following his release, he became active in campaigning against miscarriages of justice generally. He subsequently started a removal business called Small Moves, undertaking small moves and van hire in London. Although his business did well at the beginning, he subsequently began to experience interference with his business telephone calls. He alleged that local calls to his telephone were not being put through to him and that he was receiving a number of time-wasting hoax calls. The applicant suspected that this was because his mail, telephone and email communications were being intercepted. As a result of the interference, the applicant's business began to suffer.

7. The applicant believed that the interception of his communications was directly linked to his high profile case and his subsequent involvement in campaigning against miscarriages of justice. He alleged that the police and security services were continually and unlawfully renewing an interception warrant – originally authorised for the criminal proceedings against him – in order to intimidate him and undermine his business activities.

B. Domestic proceedings

8. On 10 July 2000 the applicant made subject access requests to MI5 and GCHQ (the United Kingdom's intelligence agencies responsible for national security) under the Data Protection Act 1998 ("DPA" – see paragraphs 21 to 22 below). The object of the requests was to discover whether information about him was being processed by the agencies and to obtain access to the content of the information. Both requests were refused on the basis that the information requested was exempt from the disclosure requirements of the 1998 Act on the grounds of national security under certificates issued by the Secretary of State on 22 July 2000 (MI5) and 30 July 2000 (GCHQ).

9. On 6 July 2001 the applicant lodged two complaints with the Investigatory Powers Tribunal ("IPT"). First, the applicant complained under sections 65(2)(b) and 65(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA" – see paragraphs 25 to 80 below) that his communications were being intercepted in "challengeable circumstances", within the meaning of section 65(7) RIPA (i.e. under an interception warrant or in circumstances in which there ought to have been an interception warrant or where consideration ought to have been given to obtaining an interception warrant). Second, the applicant complained under sections 6(1) and 7(1) of the Human Rights Act 1998 ("HRA") and section 65(2)(a) RIPA that there was an unlawful interference with his rights under Article 8 of the Convention.

10. The applicant's Grounds of Claim and Complaint outlined the grounds for bringing the proceedings as follows:

> "4(a) That the authorities' conduct was, and is, incompatible with his rights under Article 8 of the Convention and a violation of equivalent rights of his at common law. Such conduct is unlawful as a result of HRA s. 6(1) and forms the basis for a complaint under RIPA s. 65.
>
> (b) To the extent any such conduct purports to have the authority of a warrant issued or renewed under RIPA Part I or the corresponding predecessor provisions of the Interception of Communications Act 1985 ("IOCA"), the issue and renewal of that warrant, as well as the conduct itself, has at all times lacked the necessary justification, whether under the express provisions of RIPA Part I (or IOCA), Article 8(2) of the Convention, or the general law.
>
> (c) Moreover the authorities' conduct was and is unlawful because in breach of the requirements of the Data Protection Act 1998 ("DPA"). Conduct in breach of those requirements takes place in challengeable circumstances under RIPA s. 65(4) and (7) and is also incompatible with the Complainant's rights under Article 8 of the Convention.
>
> 5. In addition, the Complainant relies in these proceedings on his right to a fair hearing under Article 6(1) of the Convention. In light of that right, the Complainant makes certain submissions about the way in which these proceedings ought to be conducted ..."

11. The applicant requested specific directions regarding the conduct of the proceedings in order to ensure the protection of his Convention rights under Article 6 § 1. In particular, he requested that his arguments and evidence be presented at an oral hearing; that all hearings be conducted in public; that there be mutual disclosure and inspection between the parties of all witness statements and evidence upon which parties sought to rely and exchange of skeleton arguments in relation to planned legal submissions; that evidence of each party be heard in the presence of the other party or their legal representatives, with oral evidence being open to cross-examination by the other party; that any opinion received from a Commissioner be disclosed to the parties, who would have the opportunity to make oral representations in light of it; that each party be able to apply for a derogation from any of the above in relation to a particular piece of evidence; and that, following its final determination, the IPT state its findings and give reasons for its conclusions on each relevant issue. He argued that to the extent that the IPT's rules of procedure (see paragraphs 84 to 87 below) prevented the directions sought, they were incompatible with his right to a fair hearing.

12. The Grounds of Claim and Complaint referred to the applicant's belief that his communications were being intercepted and that any warrant in place was being continually renewed.

13. Paragraph 13 of the Grounds of Claim and Complaint noted:

> "So far as the proceedings are brought in reliance on HRA s. 7(1)(a) or (b), the Complainant submits that:
>
> (a) The interception, and retention or other processing of intercept product, by any of the Respondents amounts to an interference with the Complainant's right to respect for private life and correspondence protected by Article 8(1) of the Convention;
>
> (b) The interception and processing have at no time been in accordance with the law as required by Article 8(2);
>
> (c) The interception and its purported authorisation (if any), and processing, have at no time been justified as necessary in a democratic society as required by Article 8(2)."

14. Paragraph 14 of the Grounds of Claim and Complaint expanded on the applicant's submissions:

> "In particular, the Complainant submits that:
>
> (a) the proper inference from the circumstances described by the Complainant, amplified by the refusal of the [authorities] to deny the activities alleged, is that it is established on the balance of probabilities that the interception and processing took place. At minimum there is a reasonable likelihood that interception and processing ... has taken place and continues to take place (*Hewitt and Harman v. UK*, 12175/86, EComHR Report 9.5.89, paras. 26-32).
>
> (b) The interception is not in accordance with the law so far as involving a breach of any requirement of the DPA (including the Data Protection Principles) ...

(c) The complainant poses no risk to national security nor in his case could any other ground for authorising interception of his communications reasonably be considered to exist. It cannot be said that interception of his communications has at any material time been a necessary or proportionate interference ... with his rights under Article 8(1)."

15. As to remedies, the Grounds of Claim and Complaint noted the following:

"17. If the Tribunal finds that the Complainant succeeds on the claim or complaint, it is asked to make ... :

(a) a final order prohibiting each Respondent from intercepting any communication by the Complainant ... or retaining or otherwise processing the product of any such interception, except on the grounds, and subject to the procedure, provided for by RIPA Part I;

(b) an order ... quashing or cancelling any warrant or authorisation relating to any such interception;

(c) an order requiring the destruction of any product of such interception ...

(d) an award of compensation ... and/or damages ... for the loss and damage sustained by the Complainant in consequence of the matters complained of (including economic loss resulting from interference with his business communications)."

16. On 23 January 2003, the IPT, presided over by Lord Justice Mummery, issued a joint Ruling on Preliminary Issues of Law in the applicant's case together with a case involving a complaint by British-Irish Rights Watch and others in which a similar challenge to the IPT's Rules was made (see paragraphs 84 to 87 below).

17. On 9 December 2004, the IPT, again presided over by Lord Justice Mummery, issued a second ruling on preliminary issues of law in the applicant's case. In the introduction to its ruling, the IPT summarised the case before it as follows:

"1. On 6 July 2001 the Complainant made (a) a complaint to the Tribunal under the Regulation of Investigatory Powers Act ... and (b) a claim under the Human Rights Act 1998 ... in respect of alleged ongoing interception by one or more of the respondent agencies (the Security Service, GCHQ and the Commissioner of Police for the Metropolis) over a period dating back to June 1996 ...

2. The Complainant also alleges harassment, intrusive surveillance, interference with property, removal of documents, interference with a web site and e-mails and interception of privileged communications by the respondent agencies.

3. The Complainant seeks a final order prohibiting the agencies from intercepting any communication by him in the course of its transmission by means of a telecommunications system or retaining or otherwise processing the product of any such interception except on the grounds and subject to the procedure provided by RIPA Part I.

4. He also seeks an order requiring the destruction of any product of such interception held by each respondent, whether or not obtained pursuant to any warrant or authorisation; and an award of compensation under s 67(7) RIPA and/or damages sustained by the Complainant in consequence of the matters complained of."

18. The ruling dealt with a number of matters relating to the extent of its jurisdiction in respect of the applicant's complaints relating to conduct prior to the entry into force of RIPA.

19. Following its ruling of 9 December 2004, the IPT proceeded to examine the applicant's specific complaints in private.

20. On 17 January 2005, the IPT notified the applicant that no determination had been made in his favour in respect of his complaints. This meant either that there had been no interception or that any interception which took place was lawful.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. Applicable legislation

1. Subject access requests under the Data Protection Act ("DPA") 1998

21. Section 7(1) DPA grants individuals the right to request details of any information about them held by persons or organisations which record, store, or process personal data.

22. Under section 28 DPA, personal data is exempt from disclosure under section 7(1) if an exemption is required for the purpose of safeguarding national security.

2. The Human Rights Act 1998

23. The HRA incorporates the Convention into United Kingdom law. Section 6(1) provides that it is unlawful for a public authority to act in a way which is incompatible with a Convention right, except where it is constrained to act in that way as a result of primary legislation which cannot be interpreted so as to be compatible with Convention rights. Under section 7(1), a person claiming that a public authority has acted unlawfully under section 6(1) may bring proceedings against it in the appropriate court or rely on the Convention right in any legal proceedings.

24. Under section 4(2), if a court is satisfied that a provision of primary legislation is incompatible with a Convention right, it may make a declaration of that incompatibility. "Court", in section 4, is defined as meaning the Supreme Court; the Judicial Committee of the Privy Council; the Court Martial Appeal Court; in Scotland, the High Court of Justiciary (sitting otherwise than as a trial court) or the Court of Session; or in England and Wales or Northern Ireland, the High Court or the Court of Appeal. Section 4(6) clarifies that a declaration of incompatibility does not affect the validity, continuing operation or enforcement of the legislative provision in question and is not binding on the parties to the proceedings in which it is made.

3. Interception warrants

25. Since 2 October 2000, the interception of communications has been regulated by the Regulation of Investigatory Powers Act 2000 ("RIPA"). The explanatory notes which accompany RIPA explain that the main purpose of RIPA is to ensure that investigatory powers are exercised in accordance with human rights.

26. Section 71 RIPA provides for the adoption of codes of practice by the Secretary of State in relation to the exercise and performance of his powers and duties under the Act. Draft codes of practice must be laid before Parliament and are public documents. They can only enter into force in accordance with an order of the Secretary of State. The Secretary of State can only make such an order if a draft of the order has been laid before Parliament and approved by a resolution of each House.

27. Under section 72(1) RIPA, a person exercising or performing any power or duty relating to interception of communications must have regard to the relevant provisions of a code of practice. The provisions of a code of practice may, in appropriate circumstances, be taken into account by courts and tribunals under section 72(4) RIPA.

28. The Interception of Communications Code of Practice ("the Code") entered into force on 1 July 2002. It is now available on the Home Office website.

a. The issue of an interception warrant

29. Interception is permitted in several cases, exhaustively listed in section 1(5) RIPA. Section 1(5)(b), the relevant provision in the present case, provides that interception is lawful if authorised by an interception warrant. Any unlawful interception is a criminal offence under section 1(1).

30. Section 2(2) defines "interception" as follows:

> "For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he–
>
> (a) so modifies or interferes with the system, or its operation,
>
> (b) so monitors transmissions made by means of the system, or
>
> (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,
>
> as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."

31. Section 5(1) allows the Secretary of State to issue a warrant authorising the interception of the communications described in the warrant. Under section 5(2), no warrant for interception of internal communications (i.e. communications within the United Kingdom) shall be issued unless the Secretary of State 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.

32. Section 5(3) provides:

"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; [or]

(c) for the purpose of safeguarding the economic well-being of the United Kingdom ..."

33. The term "national security" is not defined in RIPA. However, it has been clarified by the Interception of Communications Commissioner appointed under RIPA's predecessor (the Interception of Communications Act 1985) who, in his 1986 report, stated that he had adopted the following definition:

"[activities] which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means."

34. Section 81(2)(b) RIPA defines "serious crime" as crime which satisfies one of the following criteria:

"(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;

(b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose."

35. Section 81(5) provides:

"For the purposes of this Act detecting crime shall be taken to include–

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed;

and any reference in this Act to preventing or detecting serious crime shall be construed accordingly ..."

36. Under section 5(4), the Secretary of State must, when assessing whether the requirements in section 5(2) are met, consider whether the information sought to be obtained under the warrant could reasonably be obtained by other means.

37. Section 5(5) provides that a warrant shall not be considered necessary for the purpose of safeguarding the economic well-being of the United Kingdom unless the information which it is thought necessary to

obtain is information relating to the acts or intentions of persons outside the British Islands.

38. Section 7(2)(a) requires the Secretary of State personally to issue all warrants of the nature at issue in the present case, except in cases of urgency where he must nonetheless personally authorise the issuing of the warrant. Section 6(2) provides an exhaustive list of those who may apply for an interception warrant, including the heads of national intelligence bodies, heads of police forces and the Customs and Excise Commissioners.

39. Paragraphs 2.4 to 2.5 of the Code provide additional guidance on the application of the proportionality and necessity test in section 5(2):

> "2.4 Obtaining a warrant under the Act will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary on one or more of the statutory grounds set out in section 5(3) of the Act. This requires him to believe that it is necessary to undertake the interception which is to be authorised for a particular purpose falling within the relevant statutory ground.
>
> 2.5 Then, if the interception is necessary, the Secretary of State must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means. Further, all interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair."

b. The contents of an application and an interception warrant

40. Section 8 sets out the requirements as to the contents of an interception warrant as regards the identification of the communications to be intercepted:

> "(1) An interception warrant must name or describe either–
>
> (a) one person as the interception subject; or
>
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.
>
> (2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules 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.
>
> (3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include–
>
> (a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or
>
> (b) communications originating on, or intended for transmission to, the premises so named or described."

41. Paragraph 4.2 of the Code provides:

"An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. 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 the 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 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."

c. Safeguards

42. Section 15 RIPA is entitled "Restrictions on use of intercepted material etc." and provides, insofar as relevant to internal communications, as follows:

"(1) ... it shall be the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing–

(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data;

...

(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following–

(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,

(b) the extent to which any of the material or data is disclosed or otherwise made available,

(c) the extent to which any of the material or data is copied, and

(d) the number of copies that are made,

is limited to the minimum that is necessary for the authorised purposes.

(3) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if–

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);

...

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are satisfied in relation to the intercepted material or any related communications data must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner ..."

43. Section 16 sets out extra safeguards which apply in the case of interception of external communications only.

44. Section 19 imposes a broad duty on all those involved in interception under RIPA to keep secret, among other matters, "everything in the intercepted material" (section 19(3)(e)). Under section 19(4), disclosure of such material is a criminal offence punishable by up to five years' imprisonment.

45. Paragraph 6.1 of the Code requires all material intercepted under the authority of a section 8(l) warrant to be handled in accordance with safeguards put in place by the Secretary of State under section 15 of the Act. Details of the safeguards are made available to the Commissioner (see paragraph 57 below) and any breach of the safeguards must be reported to him.

46. Paragraphs 6.4 to 6.8 of the Code provide further details of the relevant safeguards:

"**Dissemination of intercepted material**

6.4 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

6.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by

requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

Copying

6.6 Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of the Act. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

6.7 Intercepted material, 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 intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers ...

Destruction

6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of the Act."

47. Specific guidance is given as to the vetting of those involved in intercept activities in paragraph 6.9 of the Code:

"6.9 Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance."

48. The Government's policy on security vetting was announced to Parliament by the Prime Minister on 15 December 1994. In his statement, the Prime Minister explained the procedure for security vetting and the kinds of activities which would lead to the exclusion of an individual from participation in work vital to the interests of the State.

49. The Security Service Act 1989 and the Intelligence Services Act 1994 impose further obligations on the heads of the security and intelligence services to ensure the security of information in their possession.

d. Duration of an interception warrant

50. Section 9(1)(a) provides that an interception warrant for internal communications ceases to have effect at the end of the "relevant period" The "relevant period" is defined in section 9(6) as:

"(a) in relation to an unrenewed warrant issued in a case [issued] under the hand of a senior official, ... the period ending with the fifth working day following the day of the warrant's issue;

(b) in relation to a renewed warrant the latest renewal of which was by an instrument endorsed under the hand of the Secretary of State with a statement that the renewal is believed to be necessary on grounds falling within section 5(3)(a) [national security] or (c) [economic well-being], ... the period of six months beginning with the day of the warrant's renewal; and

(c) in all other cases, ... the period of three months beginning with the day of the warrant's issue or, in the case of a warrant that has been renewed, of its latest renewal."

51. Section 9(1)(b) provides that an interception warrant may be renewed by the Secretary of State at any time before its expiry where he believes that the warrant continues to be necessary on grounds falling within section 5(3).

52. The Secretary of State is required under Section 9(3) to cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3).

53. Section 10(2) imposes an obligation on the Secretary of State to delete any factor set out in a schedule to an interception warrant which he considers is no longer relevant for identifying communications which, in the case of that warrant, are likely to be or to include communications from, or intended for, the interception subject.

54. Paragraph 4.13 of the Code provides:

"The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals must be made to the Secretary of State and should contain an update of the matters outlined in paragraph 4.2 above. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of the purposes in section 5(3)."

55. Paragraph 4.16 of the Code provides:

"The Secretary of State is under a duty to cancel an interception warrant if, at any time before its expiry date, he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of the Act. Intercepting agencies will therefore need to keep their warrants under continuous review. In practice, cancellation instruments will be signed by a senior official on his behalf."

e. Duty to keep records

56. Paragraph 4.18 of the Code imposes record-keeping obligations on intercepting agencies and provides:

"The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State based his decision, and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he may require:

- all applications made for warrants complying with section 8(l) and applications made for the renewal of such warrants;
- all warrants, and renewals and copies of schedule modifications (if any);
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the dates on which interception is started and stopped."

4. The Commissioner

a. Appointment and functions

57. Section 57 RIPA provides that the Prime Minister shall appoint an Interception of Communications Commissioner ("the Commissioner"). He must be a person who holds or has held high judicial office. The Commissioner is appointed for a three-year, renewable term. To date, there have been two Commissioners appointed under RIPA. Both are former judges of the Court of Appeal.

58. The Commissioner's functions include to keep under review the exercise and performance by the Secretary of State of powers and duties in relation to interception conferred or imposed on him by RIPA; the exercise and performance of powers and duties in relation to interception by the persons on whom such powers or duties are conferred or imposed; and the adequacy of the arrangements by virtue of which the duty which is imposed on the Secretary of State by section 15 (safeguards – see paragraph 42 above) is sought to be discharged.

59. Section 58 RIPA places a duty on those involved in the authorisation or execution of interception warrants to disclose to the Commissioner all documents and information which he requires in order to carry out his functions. As noted above (see paragraph 56), the Code requires intercepting agencies to keep accurate and comprehensive records for this purpose.

60. In his 2005-2006 report, the Commissioner described his inspections as follows:

> "12. In accordance with [my] duties I have continued my practice of making twice yearly visits to ... the intercepting agencies and the departments of the Secretaries of State/Ministers which issue the warrants. Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since my previous visit. I then select, largely at random, a sample of warrants for inspection. In the course of my visit I satisfy myself that those warrants fully meet the requirements of RIPA, that proper procedures have been followed and that the relevant safeguards and Codes of Practice have been followed. During each visit I review each of the files and the supporting documents and, when necessary, discuss the cases with the officers concerned. I can view the product of interception. It is of first importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

13. I continue to be impressed by the quality, dedication and enthusiasm of the personnel carrying out this work on behalf of the Government and the people of the United Kingdom. They have a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards ..."

61. The Commissioner is required to report to the Prime Minister if he finds that there has been a violation of the provisions of RIPA or if he considers that the safeguards under section 15 have proved inadequate (sections 58(2) and (3) RIPA). The Commissioner must also make an annual report to the Prime Minister regarding the exercise of his functions (section 58(4)). Under section 58(6), the Prime Minister must lay the annual report of the Commissioner before Parliament. Finally, the Commissioner is required to assist the IPT with any request for information or advice it may make (section 57(3) and paragraph 78 below)).

b. Relevant extracts of reports

62. In his 2000 report, the Commissioner noted, as regards the discharge of their duties by the Secretaries of State:

"12. ... I have been impressed with the care that they take with their warrantry work, which is very time consuming, to ensure that warrants are issued only in appropriate cases and, in particular, in ensuring that the conduct authorised is proportionate to what is sought to be achieved by the intercepts."

63. At paragraph 15, on the question of safeguards, he said:

"... my advice and approval were sought and given in respect of the safeguard documents either before or shortly after 2 October 2000. The Home Secretary also sought my advice in relation to them and they were approved by him ..."

64. As to the need for secret surveillance powers, the Commissioner commented:

"45. The interception of communications is, as my predecessors have expressed in their Report, an invaluable weapon for the purpose set out in section 5(3) of RIPA and, in particular, in the battle against serious crime ..."

65. In his report for 2001, the Commissioner noted:

"10. Many members of the public are suspicious about the interception of communications, and some believe that their own conversations are subject to unlawful interception by the security, intelligence or law enforcement agencies ... In my oversight work I am conscious of these concerns. However, I am as satisfied as I can be that the concerns are, in fact, unfounded. Interception of an individual's communications can take place only after a Secretary of State has granted a warrant and the warrant can be granted on strictly limited grounds set out in Section 5 of RIPA, essentially the interests of national security and the prevention or detection of serious crime. Of course, it would theoretically be possible to circumvent this procedure, but there are in place extensive safeguards to ensure that this cannot happen, and it is an important part of my work to ensure that these are in place, and that they are observed. Furthermore, any attempt to get round the procedures which provide for legal interception would, by reason of the safeguards, involve a major

conspiracy within the agency concerned which I believe would, for practical purposes, be impossible. I am as satisfied as it is possible to be that deliberate unlawful interception of communications of the citizen does not take place ..."

66. He said of the section 15 safeguards:

"31. In addressing the safeguards contained within section 15 of RIPA, GCHQ developed a new set of internal compliance documentation for staff, together with an extensive training programme that covered staff responsibilities under both RIPA and the Human Rights Act. This compliance documentation was submitted to the Foreign Secretary who was satisfied that it described and governed the arrangements required under section 15. I have also been told it also constituted the written record of the arrangements required to be put in place by the Director, GCHQ, under section 4(2)(a) of the Intelligence Services Act 1994 (to ensure that no information is obtained or disclosed by GCHQ except so far as is necessary for its statutory functions). In discharging my functions under section 57(1)(d), I examined the documentation and the processes which underpin it and satisfied myself that adequate arrangements existed for the discharge of the Foreign Secretary's duties under section 15 of RIPA. Of course, GCHQ recognises that its compliance processes must evolve over time, particularly as they become more familiar with the intricacies of the new legislation and develop new working practices, and that the process of staff education remains a continuing one. To this end, GCHQ has developed further training programmes and is issuing revised compliance documentation as part of the ongoing process (see also ... paragraph 56 under Safeguards).

32. In advance of the coming into force of RIPA, GCHQ approached me as to the warrants it would seek after that date and provided a detailed analysis as to how those warrants would be structured – this was helpful as it gave me an insight into how GCHQ saw the workings of RIPA/Human Rights Act and permitted me to comment in advance. Since the commencement of RIPA, in reviewing warrants I have looked carefully at the factors to be considered by the Secretary of State when determining whether to issue an interception warrant, and especially the new requirement to consider 'proportionality' under section [5(2)(b)] of RIPA."

67. Again, he commented on the diligence of the authorities in carrying out their duties under the Act:

"56. Sections 15 and 16 of RIPA lay a duty on the Secretary of State to ensure that arrangements are in force as safeguards in relation to dissemination, disclosure, copying, storage, and destruction etc., of intercepted material. These sections require careful and detailed safeguards to be drafted by each of the agencies referred to earlier in this Report and for those safeguards to be approved by the Secretary of State. This had been done. I have been impressed by the care with which these documents have been drawn up, reviewed and updated in the light of technical and administrative developments. Those involved in the interception process are aware of the invasive nature of this technique, and care is taken to ensure that intrusions of privacy are kept to the minimum. There is another incentive to agencies to ensure that these documents remain effective in that the value of interception would be greatly diminished as a covert intelligence tool should its existence and methodology become too widely known. The sections 15 and 16 requirements are very important. I am satisfied that the agencies are operating effectively within their safeguards."

68. The Commissioner's 2002 report noted:

"18. ... As I mentioned in my last Report I have been impressed by the care with which [the safeguard] documents have been drawn up. My advice and approval was sought for the documents and I am approached to agree amendments to the safeguards when they are updated in light of technical and administrative developments."

69. This was repeated in paragraph 16 of his 2004 report.

70. In his 2005-2006 report, the Commissioner explained his role as follows:

"7. ... essentially I see the role of Commissioner as encompassing these primary headings:

(a) To protect people in the United Kingdom from any unlawful intrusion of their privacy. This is provided for by Article 8 of the European Convention on Human Rights. I must be diligent to ensure that this does not happen, and alert to ensure that there are systems in place so that this does not and cannot happen. Over the long period that I have held my present post, I have found no evidence whatsoever of any desire within the Intelligence or the Law Enforcement Agencies in this field to act wrongfully or unlawfully. On the contrary, I have found a palpable desire on the part of all these Agencies to ensure that they do act completely within the four walls of the law. To this end, they welcome the oversight of the Commissioner and over the years have frequently sought my advice on issues that have arisen, and they have invariably accepted it. In any event, I believe that the legislation together with the safeguards and Codes of Practice that are in place make it technically virtually impossible to deliberately intercept a citizen's communications unlawfully with intent to avoid legal requirements.

(b) To assist the Agencies to do the work entrusted to them and, bearing in mind the number of organisations that I am now required to oversee, this occurs quite frequently. My work is, of course, limited to the legal as opposed to the operational aspects of their work. They take great care with their work and I have been impressed by its quality.

(c) To ensure that proper safeguards and Codes of Practice are in place to protect the public and the Agencies themselves. These have to be approved by the Secretaries of State. But every Secretary of State with whom I have worked has required to be informed as to whether the Commissioner has approved them before he or she is willing to do so.

(d) To advise Ministers, and Government Departments, in relation to issues arising on the interception of communications, the acquisition and disclosure of communications data, to approve the safeguards documents and the Codes of Practice."

71. The Commissioner said of the Secretaries of State whom he had met in the previous year:

"14. It is clear to me that each of them gives a substantial amount of time and takes considerable care to satisfy himself or herself that warrants are necessary for the authorised purposes, and that what is proposed is proportionate. If the Secretary of State wishes to have further information in order to be satisfied that he or she should grant the warrant then it is requested and given. Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of

necessity or proportionality are not met, and the agencies are well aware that the Secretary of State does not act as a 'rubber stamp'."

72. In his 2007 report, The Commissioner commented on the importance of interception powers in tackling terrorism and serious crime:

"2.9 I continue to be impressed as to how interception has contributed to a number of striking successes during 2007. It has played a key role in numerous operations including, for example, the prevention of murders, tackling large-scale drug importations, evasion of Excise duty, people smuggling, gathering intelligence both within the United Kingdom and overseas on terrorist and various extremist organisations, confiscation of firearms, serious violent crime and terrorism. I have provided fully detailed examples in the Confidential Annex to this Report. I think it is very important that the public is re-assured as to the benefits of this highly intrusive investigative tool particularly in light of the on-going debate about whether or not intercept product should be used as evidence in a court of law.

...

7.1 As I said in my first Report last year, the interception of communications is an invaluable weapon for the purposes set out in section 5(3) of RIPA. It has continued to play a vital part in the battle against terrorism and serious crime, and one that would not have been achieved by other means ..."

73. As regards errors by the relevant agencies in the application of RIPA's provisions, he noted:

"2.10 Twenty-four interception errors and breaches have been reported to me during the course of 2007. This is the same number of errors reported in my first Annual Report (which was for a shorter period) and is a significant decrease in the number reported by my predecessor. I consider the number of errors to be too high. By way of example, details of some of these errors are recorded below. It is very important from the point of view of the public that I stress that none of the breaches or errors were deliberate, that all were caused by human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. The most common cause of error tends to be the simple transposition of numbers by mistake e.g., 1965 instead of 1956. The examples that I give are typical of the totality and are anonymous so far as the targets are concerned. Full details of all the errors and breaches are set out in the Confidential Annex."

74. According to the statistics in the report, on 31 December 2007, 929 interception warrants issued by the Home Secretary were in force.

5. The Investigatory Powers Tribunal

a. The establishment of the IPT, its powers and its procedures

75. The IPT was established under section 65(1) RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA. Members of the tribunal must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing. Any person may bring a claim before the IPT and, save for

vexatious or frivolous applications, the IPT must determine all claims brought before it (sections 67(1), (4) and (5) RIPA).

76. Section 65(2) provides that the IPT is the only appropriate forum in relation to proceedings for acts incompatible with Convention rights which are proceedings against any of the intelligence services; and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. Sections 67(2) and 67(3)(c) provide that the IPT is to apply the principles applicable by a court on an application for judicial review.

77. Under section 67(8) RIPA, there is no appeal from a decision of the IPT "except to such extent as the Secretary of State may by order otherwise provide". No order has been passed by the Secretary of State.

78. Under section 68(2), the IPT has the power to require a relevant Commissioner to provide it with all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the IPT) as it thinks fit. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require.

79. Section 68(4) deals with reasons for the IPT's decisions and provides that:

> "Where the Tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of section 69(2)(i)) shall be confined, as the case may be, to either—
>
> (a) a statement that they have made a determination in his favour; or
>
> (b) a statement that no determination has been made in his favour."

80. The IPT has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any section 8(1) warrant and orders requiring the destruction of any records obtained under a section 8(1) warrant (section 67(7) RIPA). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

b. The power to adopt rules of procedure

81. As to procedure, section 68(1) provides as follows:

> "Subject to any rules made under section 69, the Tribunal shall be entitled to determine their own procedure in relation to any proceedings, complaint or reference brought before or made to them."

82. Section 69(1) RIPA provides that the Secretary of State may make rules regulating any matters preliminary or incidental to, or arising out of,

the hearing or consideration of any proceedings before it. Under section 69(2), such rules may:

> "(c) prescribe the form and manner in which proceedings are to be brought before the Tribunal or a complaint or reference is to be made to the Tribunal;
>
> ...
>
> (f) prescribe the forms of hearing or consideration to be adopted by the Tribunal in relation to particular proceedings, complaints or references ... ;
>
> (g) prescribe the practice and procedure to be followed on, or in connection with, the hearing or consideration of any proceedings, complaint or reference (including, where applicable, the mode and burden of proof and the admissibility of evidence);
>
> (h) prescribe orders that may be made by the Tribunal under section 67(6) or (7);
>
> (i) require information about any determination, award, order or other decision made by the Tribunal in relation to any proceedings, complaint or reference to be provided (in addition to any statement under section 68(4)) to the person who brought the proceedings or made the complaint or reference, or to the person representing his interests."

83. Section 69(6) provides that in making the rules the Secretary of State shall have regard to:

> "(a) the need to secure that matters which are the subject of proceedings, complaints or references brought before or made to the Tribunal are properly heard and considered; and
>
> (b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services."

c. The Rules

84. The Secretary of State has adopted rules to govern the procedure before the IPT in the form of the Investigatory Powers Tribunal Rules 2000 ("the Rules"). The Rules cover various aspects of the procedure before the IPT. As regards disclosure of information, Rule 6 provides:

> "(1) The Tribunal shall carry out their functions in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.
>
> (2) Without prejudice to this general duty, but subject to paragraphs (3) and (4), the Tribunal may not disclose to the complainant or to any other person:
>
> (a) the fact that the Tribunal have held, or propose to hold, an oral hearing under rule 9(4);
>
> (b) any information or document disclosed or provided to the Tribunal in the course of that hearing, or the identity of any witness at that hearing;

(c) any information or document otherwise disclosed or provided to the Tribunal by any person pursuant to section 68(6) of the Act (or provided voluntarily by a person specified in section 68(7));

(d) any information or opinion provided to the Tribunal by a Commissioner pursuant to section 68(2) of the Act;

(e) the fact that any information, document, identity or opinion has been disclosed or provided in the circumstances mentioned in sub-paragraphs (b) to (d).

(3) The Tribunal may disclose anything described in paragraph (2) with the consent of:

(a) in the case of sub-paragraph (a), the person required to attend the hearing;

(b) in the case of sub-paragraphs (b) and (c), the witness in question or the person who disclosed or provided the information or document;

(c) in the case of sub-paragraph (d), the Commissioner in question and, to the extent that the information or opinion includes information provided to the Commissioner by another person, that other person;

(d) in the case of sub-paragraph (e), the person whose consent is required under this rule for disclosure of the information, document or opinion in question.

(4) The Tribunal may also disclose anything described in paragraph (2) as part of the information provided to the complainant under rule 13(2), subject to the restrictions contained in rule 13(4) and (5).

(5) The Tribunal may not order any person to disclose any information or document which the Tribunal themselves would be prohibited from disclosing by virtue of this rule, had the information or document been disclosed or provided to them by that person.

(6) The Tribunal may not, without the consent of the complainant, disclose to any person holding office under the Crown (except a Commissioner) or to any other person anything to which paragraph (7) applies.

(7) This paragraph applies to any information or document disclosed or provided to the Tribunal by or on behalf of the complainant, except for ... statements [as to the complainant's name, address and date of birth and the public authority against which the proceedings are brought].”

85. Rule 9 deals with the forms of hearings and consideration of the complaint:

“(1) The Tribunal's power to determine their own procedure in relation to section 7 proceedings and complaints shall be subject to this rule.

(2) The Tribunal shall be under no duty to hold oral hearings, but they may do so in accordance with this rule (and not otherwise).

(3) The Tribunal may hold, at any stage of their consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses.

(4) The Tribunal may hold separate oral hearings which:

(a) the person whose conduct is the subject of the complaint,

(b) the public authority against which the section 7 proceedings are brought, or

(c) any other person specified in section 68(7) of the Act,

may be required to attend and at which that person or authority may make representations, give evidence and call witnesses.

(5) Within a period notified by the Tribunal for the purpose of this rule, the complainant, person or authority in question must inform the Tribunal of any witnesses he or it intends to call; and no other witnesses may be called without the leave of the Tribunal.

(6) The Tribunal's proceedings, including any oral hearings, shall be conducted in private."

86. The taking of evidence is addressed in Rule 11:

"(1) The Tribunal may receive evidence in any form, and may receive evidence that would not be admissible in a court of law.

(2) The Tribunal may require a witness to give evidence on oath.

(3) No person shall be compelled to give evidence at an oral hearing under rule 9(3)."

87. Finally, Rule 13 provides guidance on notification to the complainant of the IPT's findings:

"(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.

(2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.

...

(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).

(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal."

d. The practice of the IPT

88. In its joint ruling on preliminary issues of law (see paragraph 16 above), the IPT clarified a number of aspects of its procedure. The IPT sat, for the first time, in public. As regards the IPT procedures and the importance of the cases before it, the IPT noted:

"10. The challenge to rule 9(6) [requiring oral hearings to be held in private] and to most of the other rules governing the basic procedures of the Tribunal have made this the most significant case ever to come before the Tribunal. The Tribunal are left in no doubt that their rulings on the legal issues formulated by the parties have potentially important consequences for dealing with and determining these and future proceedings and complaints. Counsel and those instructing them were encouraged to argue all the issues in detail, in writing as well as at the oral hearings held over a period of three days in July and August 2002. At the end of September 2002 the written submissions were completed when the parties provided, at the request of the Tribunal, final comments on how the Rules ought, if permissible and appropriate, to

be revised and applied by the Tribunal, in the event of a ruling that one or more of the Rules are incompatible with Convention rights and/or *ultra vires*."

89. The IPT concluded (at paragraph 12) that:

"... (a) the hearing of the preliminary issues should have been conducted in public, and not in private as stated in rule 9(6); (b) the reasons for the legal rulings should be made public; and (c) in all other respects the Rules are valid and binding on the Tribunal and are compatible with Articles 6, 8 and 10 of the Convention."

90. Specifically on the applicability of Article 6 § 1 to the proceedings before it, the IPT found:

"85. The conclusion of the Tribunal is that Article 6 applies to a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves 'the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)."

91. After a review of the Court's case-law on the existence of a "civil right", the IPT explained the reasons for its conclusions:

"95. The Tribunal agree with the Respondents that there is a sense in which the claims and complaints brought by virtue of s 65(2) of RIPA fall within the area of public law. They arise out of the alleged exercise of very wide discretionary, investigatory, state powers by public authorities, such as the intelligence and security agencies and the police. They are concerned with matters of national security, of public order, safety and welfare. The function of the Tribunal is to investigate and review the lawfulness of the exercise of such powers. This is no doubt intended to ensure that the authorities comply with their relevant public law duties, such as by obtaining appropriate warrants and authorisations to carry out interception and surveillance.

96. The public law element is reinforced by the directions to the Tribunal in sections 67(2) and 67(3)(c) of RIPA to apply to the determinations the same principles as would be applied by a court in judicial review proceedings. Such proceedings are concerned with the procedural and substantive legality of decisions and actions of public authorities.

97. The fact that activities, such as interception of communications and surveillance, may also impact on the Convention rights of individuals, such as the right to respect for private life and communications in Article 8, does not of itself necessarily mean that the Tribunal make determinations of civil rights ...

98. Further, the power of the Tribunal to make an award of compensation does not necessarily demonstrate that the Tribunal determine civil rights ...

99. Applying the approach in the Strasbourg cases that account should be taken of the content of the rights in question and of the effect of the relevant decision on them ..., the Tribunal conclude that the public law or public order aspects of the claims and complaints to the Tribunal do not predominate and are not decisive of the juristic character of the determinations of the Tribunal. Those determinations have a sufficiently decisive impact on the private law rights of individuals and organisations to attract the application of Article 6.

100. The jurisdiction of the Tribunal is invoked by the initiation of claims and complaints by persons wishing to protect, and to obtain redress for alleged infringements of, their underlying rights of confidentiality and of privacy for person,

property and communications. There is a broad measure of protection for such rights in English private law in the torts of trespass to person and property, in the tort of nuisance, in the tort of misfeasance in a public office, in the statutory protection from harassment and in the developing equitable doctrine of breach of confidence ...

101. Since 2 October 2000 there has been added statutory protection for invasion of Article 8 rights by public authorities. This follows from the duties imposed on public authorities by section 6 and the rights conferred on victims by section 7 of the [Human Rights Act]. The concept of 'civil rights and obligations' is a fair and reasonable description of those common law and statutory rights and obligations, which form the legal foundation of a person's right to bring claims and make complaints by virtue of section 65.

102. The fact that the alleged infringements of those rights is by public authorities in purported discretionary exercise of administrative investigatory powers does not detract from the 'civil' nature of the rights and obligations in issue ...

...

107. For all practical purposes the Tribunal is also the only forum for the effective investigation and determination of complaints and for granting redress for them where appropriate ...

108. In brief, viewing the concept of determination of 'civil rights' in the round and in the light of the Strasbourg decisions, the Tribunal conclude that RIPA, which puts all interception, surveillance and similar intelligence gathering powers on a statutory footing, confers, as part of that special framework, additional 'civil rights' on persons affected by the unlawful exercise of those powers. It does so by establishing a single specialised Tribunal for the judicial determination and redress of grievances arising from the unlawful use of investigatory powers."

92. As to the proper construction of Rule 9 regarding oral hearings, the IPT found:

"157. The language of rule 9(2) is clear:

'The Tribunal shall be under no duty to hold oral hearings but may do so in accordance with this rule (and not otherwise).'

158. Oral hearings are in the discretion of the Tribunal. They do not have to hold them, but they may, if they so wish, do so in accordance with Rule 9.

159. In the exercise of their discretion the Tribunal 'may hold separate oral hearings.' That exercise of discretion, which would be a departure from normal adversarial procedures, is expressly authorised by rule 9(4).

160. The Tribunal should explain that, contrary to the views apparently held by the Complainants' advisers, the discretion in rule 9(4) neither expressly nor impliedly precludes the Tribunal from exercising their general discretion under rule 9(2) to hold inter partes oral hearings. It is accepted by the Respondents that the Tribunal may, in their discretion, direct joint or collective oral hearings to take place. That discretion was in fact exercised in relation to this very hearing. The exercise of discretion must take into account the relevant provisions of other rules, in particular the Tribunal's general duty under rule 6(1) to prevent the potentially harmful disclosure of sensitive information in the carrying out of their functions. As already explained, this hearing has neither required nor involved the disclosure of any such information or documents emanating from the Complainants, the Respondents or anyone else. The hearing has

only been concerned with undiluted legal argument about the procedure of the Tribunal.

161. The Tribunal have reached the conclusion that the absence from the Rules of an absolute right to either an inter partes oral hearing, or, failing that, to a separate oral hearing in every case is within the rule-making power in section 69(1). It is also compatible with the Convention rights under Article 6, 8 and 10. Oral hearings involving evidence or a consideration of the substantive merits of a claim or complaint run the risk of breaching the [neither confirm nor deny] policy or other aspects of national security and the public interest. It is necessary to provide safeguards against that. The conferring of a discretion on the Tribunal to decide when there should be oral hearings and what form they should take is a proportionate response to the need for safeguards, against which the tribunal, as a judicial body, can balance the Complainants' interests in a fair trial and open justice according to the circumstances of the particular case."

93. Regarding Rule 9(6) which stipulates that oral hearings must be held in private, the IPT held:

"163. The language of rule 9(6) is clear and unqualified.

'The Tribunal's proceedings, including any oral hearings, shall be conducted in private.'

164. The Tribunal are given no discretion in the matter. Rule 6(2)(a) stiffens the strictness of the rule by providing that the Tribunal may not even disclose to the Complainant or to any other person the fact that the Tribunal have held, or propose to hold, a separate oral hearing under rule 9(4). The fact of an oral hearing is kept private, even from the other party ...

...

167. ... the very fact that this rule is of an absolute blanket nature is, in the judgment of the Tribunal in the circumstances, fatal to its validity ... the Tribunal have concluded that the very width of the rule preventing any hearing of the proceedings in public goes beyond what is authorised by section 69 of RIPA.

...

171. There is no conceivable ground for requiring legal arguments on pure points of procedural law, arising on the interpretation and validity of the Rules, to be held in private ...

172. Indeed, purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of any sensitive information, should be heard in public. The public, as well as the parties, has a right to know that there is a dispute about the interpretation and validity of the relevant law and what the rival legal contentions are.

173. The result is that rule 9(6) is ultra vires section 69. It does not bind the Tribunal. The Secretary of State may exercise his discretion under section 69(1) to make fresh rules on the point, but, unless and until he does, the Tribunal may exercise their discretion under section 68(1) to hear the legal arguments in public under rule 9(3), subject to their general and specific duties, such as rule 6(1) in the Rules and in RIPA. It is appropriate to exercise that discretion to direct that the hearing of the preliminary issues shall be treated as if it had taken place under rule 9(3) in public, because such a preliminary hearing of purely legal arguments solely on procedural issues does not pose any risk to the duty of the Tribunal under rule 6(1) or to the

maintenance of the [neither confirm nor deny] policy. The transcripts of the hearing should be made available for public consumption."

94. Regarding other departures from the normal rules of adversarial procedure as regards the taking of evidence and disclosure in Rule 6, the IPT concluded:

"181. ... that these departures from the adversarial model are within the power conferred on the Secretary of State by section 69(1), as limited by section 69(6). A reasonable rule-making body, having regard to the mandatory factors in section 69(6), could properly conclude that these departures were necessary and proportionate for the purposes stated in section 69(6)(b). In the context of the factors set out in that provision and, in particular, the need to maintain the [neither confirm nor deny] policy, the procedures laid down in the Rules provide a 'fair trial' within Article 6 for the determination of the civil rights and obligations arising in claims and complaints under section 65 of RIPA.

182. They are also compatible with Convention rights in Articles 8 and 10, taking account of the exceptions for the public interest and national security in Articles 8(2) and 10(2), in particular the effective operation of the legitimate policy of [neither confirm nor deny] in relation to the use of investigatory powers. The disclosure of information is not an absolute right where there are competing interests, such as national security considerations, and it may be necessary to withhold information for that reason, provided that, as in the kind of cases coming before this Tribunal, it is strictly necessary to do so and the restriction is counterbalanced by judicial procedures which protect the interests of the Complainants ..."

95. Finally, as regards the absence of reasons following a decision that the complaint is unsuccessful, the IPT noted:

"190. The Tribunal conclude that, properly interpreted in context on ordinary principles of domestic law, rule 13 and section 68(4) of RIPA do not apply to prevent publication of the reasons for the rulings of the Tribunal on the preliminary issues on matters of procedural law, as they are not a 'determination' of the proceedings brought before them or of the complaint made to them within the meaning of those provisions. Those provisions concern decisions of the Tribunal which bring the claim or complaint to an end, either by a determination of the substantive claim or complaint on its merits ...

191. ... In the circumstances there can be publication of the reasons for legal rulings on preliminary issues, but, so far as determinations are concerned, the Tribunal are satisfied that section 68(4) and rule 13 are valid and binding and that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the [neither confirm nor deny] policy must be preserved) is necessary and justifiable."

96. In a second ruling on preliminary issues of law in the *British-Irish Rights Watch and others* case, which involved external communications (i.e. communications between the United Kingdom and abroad), the IPT issued its findings on the complaint in that case. The issue for consideration was identified as:

"3. ... whether ... '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' ..."

97. Given that the challenge in the case related solely to the lawfulness of the filtering process as set out in the RIPA legislation, the IPT issued a public ruling which explained the reasons for its findings in the case. In its ruling, it examined the relevant legislative provisions and concluded that they were sufficiently accessible and foreseeable to be in accordance with the law.

98. As the applicant's case demonstrates, once general legal issues have been determined, if the IPT is required to consider the specific facts of the case, and in particular whether interception has taken place, any such consideration will take place in private. Rule 6 prevents the applicant participating in this stage of proceedings.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

99. The applicant complained that his communications were being unlawfully intercepted in order to intimidate him and undermine his business activities, in violation of Article 8 of the Convention, which 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."

100. He further argued that the regime established under RIPA for authorising interception of internal communications did not comply with the requirements of Article 8 § 2 of the Convention.

A. Admissibility

1. The parties' submissions

a. The Government

101. The Government argued that the applicant had failed to advance a general challenge to the Convention-compliance of the RIPA provisions on interception of internal communications before the IPT, and that he had accordingly failed to exhaust domestic remedies in respect of this complaint. They pointed out that at the same time as the applicant was pursuing his complaint with the IPT, the *British-Irish Rights Watch and*

others case was also under consideration by the IPT. Pursuant to the arguments of the parties in that case, the IPT issued a general public ruling of the IPT on the compatibility of the RIPA scheme as regards external communications with Article 8 (see paragraphs 96 to 97 above). No such ruling on the subject of internal communications was issued in the applicant's case.

102. The Government emphasised that the applicant's Grounds of Claim and Complaint alleged interception of the applicant's business calls and a violation of Article 8 on the facts of the applicant's case. The Government noted that the paragraphs of the Grounds of Claim and Complaint relied upon by the applicant in his submissions to this Court to support his allegation that a general complaint was advanced were misleading. It was clear from the description of his complaint and the subsequent paragraphs particularising his claim that the reference to interception was to an alleged interception in his case, and not to interception in general, and that the complaint that the interception was not in accordance with the law related to an alleged breach of the Data Protection Act, and not to any alleged inadequacies of the RIPA regime (see paragraphs 12 and 14 above).

103. The Government submitted that Article 35 § 1 had a special significance in the context of secret surveillance, as the IPT was specifically designed to be able to consider and investigate closed materials. It had extensive powers to call for evidence from the intercepting agencies and could request assistance from the Commissioner, who had detailed working knowledge and practice of the section 8(1) warrant regime.

104. As regards the applicant's specific complaint that his communications had been unlawfully intercepted, the Government contended that the complaint was manifestly ill-founded as the applicant had failed to show that there had been an interference for the purposes of Article 8. In their submission, he had not established a reasonable likelihood, as required by the Court's case-law, that his communications had been intercepted.

105. The Government accordingly invited the Court to find both the general and the specific complaints under Article 8 inadmissible.

b. The applicant

106. The applicant refuted the suggestion that his complaint before the IPT had failed to challenge the Convention-compatibility of the RIPA regime on internal communications and that he had, therefore, failed to exhaust domestic remedies in this regard. He pointed out that one of the express grounds of his complaint to the IPT had been that "the interception and processing ha[d] at no time been in accordance with the law as required by Article 8(2)" (see paragraph 13 above). He argued that his assertion before the IPT was that any warrants issued or renewed under RIPA violated Article 8.

107. The applicant further disputed that there had been no interference in his case, maintaining that he had established a reasonable likelihood that interception had taken place and that, in any event, the mere existence of RIPA was sufficient to show an interference.

2. The Court's assessment

108. As regards the Government's objection that the applicant failed to exhaust domestic remedies, the Court considers that the summary of the applicant's case set out by the IPT in its ruling of 9 January 2004 (see paragraph 17 above) as well as the Grounds of Claim and Complaint themselves (see paragraphs 10 to 15 above) support the Government's contention that the applicant's complaint concerned only the specific allegation that his communications were actually being intercepted. Further, it can be inferred from the fact that the IPT issued a general public ruling on the compliance of the RIPA provisions on external communications with Article 8 in the *British-Irish Rights Watch and others* case (see paragraphs 96 to 97 above) that, had a similar argument in respect of internal communications been advanced by the applicant, a similar public ruling would have been issued in his case. No such ruling was handed down. The Court therefore concludes that the applicant failed to raise his arguments as regards the overall Convention-compatibility of the RIPA provisions before the IPT.

109. However, the Court recalls that where the Government claims non-exhaustion they must satisfy the Court that the remedy proposed was an effective one available in theory and in practice at the relevant time, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success (see, *inter alia*, *Akdivar and Others v. Turkey*, 16 September 1996, § 68, *Reports of Judgments and Decisions* 1996-IV; and *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006-II). While the Government rely on the *British-Irish Rights Watch and others* case to demonstrate that the IPT could have issued a general ruling on compatibility, they do not address in their submissions to the Court what benefit, if any, is gained from such a general ruling. The Court recalls that it is in principle appropriate that the national courts should initially have the opportunity to determine questions of the compatibility of domestic law with the Convention in order that the Court can have the benefit of the views of the national courts, as being in direct and continuous contact with the forces of their countries (see *Burden v. the United Kingdom* [GC], no. 13378/05, § 42, ECHR 2008-...; and *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 154, ECHR 2009-....). However, it is important to note in this case that the applicant's challenge to the RIPA provisions is a challenge to primary legislation. If the applicant had made a general complaint to the IPT, and if that complaint been upheld, the tribunal did not have the power to annul any of the RIPA provisions or

to find any interception arising under RIPA to be unlawful as a result of the incompatibility of the provisions themselves with the Convention (see paragraph 24 above). No submissions have been made to the Court as to whether the IPT is competent to make a declaration of incompatibility under section 4(2) of the Human Rights Act. However, it would appear from the wording of that provision that it is not. In any event, the practice of giving effect to the national courts' declarations of incompatibility by amendment of offending legislation is not yet sufficiently certain as to indicate that section 4 of the Human Rights Act is to be interpreted as imposing a binding obligation giving rise to a remedy which an applicant is required to exhaust (see *Burden v. the United Kingdom*, cited above, §§ 43 to 44). Accordingly, the Court considers that the applicant was not required to advance his complaint regarding the general compliance of the RIPA regime for internal communications with Article 8 § 2 before the IPT in order to satisfy the requirement under Article 35 § 1 that he exhaust domestic remedies.

110. The Court takes note of the Government's argument that Article 35 § 1 has a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information. While the extensive powers of the IPT are relevant where the tribunal is examining a specific complaint of interception in an individual case and it is necessary to investigate the factual background, their relevance to a legal complaint regarding the operation of the legislative regime is less clear. In keeping with its obligations under RIPA and the Rules (see paragraphs 83 to 84 above), the IPT is not able to disclose information to an extent, or in a manner, contrary to the public interest or prejudicial to national security or the prevention or detection of serious crime. Accordingly, it is unlikely that any further elucidation of the general operation of the interception regime and applicable safeguards, such as would assist the Court in its consideration of the compliance with the regime with the Convention, would result from a general challenge before the IPT.

111. As regards the Government's second objection that there has been no interference in the applicant's case, the Court considers that this raises serious questions of fact and of law which cannot be settled at this stage of the examination of the application but require an examination of the merits of the complaint.

112. In conclusion, the applicant's complaint under Articles 8 cannot be rejected for non-exhaustion of domestic remedies under Article 35 § 1 or as manifestly ill-founded within the meaning of Article 35 § 3. The Court notes, in addition, that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The existence of an "interference"

a. The parties' submissions

i. The applicant

113. The applicant insisted that his communications had been intercepted. He maintained that there were reasonable grounds for believing that he had been subject to interception and submitted that objectively verifiable facts supported the possibility of interception, pointing to his long campaign regarding the alleged miscarriage of justice in his case and the allegation of police impropriety made at his re-trial.

114. Noting the Government's submission that neither preventing calls from being put through nor hoax calls amounted to interception for the purposes of RIPA, the applicant emphasised that such conduct clearly amounted to an interference for the purposes of Article 8 of the Convention. In the event that RIPA did not apply to such measures, he argued that the Government had failed to indicate the alternative legal regime put in place to prevent such interference with individuals' private lives as required by the positive obligations under Article 8.

115. Finally, and in any event, relying on *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 78, ECHR 2006-XI, the applicant contended that he was not required to demonstrate that the impugned measures had actually been applied to him in order to establish an interference with his private life. He invited the Court to follow its judgment in *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 56 to 57, 1 July 2008, and find that the mere existence of a regime for surveillance measures entailed a threat of surveillance for all those to whom the legislation could be applied.

ii. The Government

116. The Government accepted that if the applicant's complaint regarding the general Convention-compatibility of the RIPA scheme was admissible, then he could claim to be a victim without having to show that he had actually been the subject of interception, However, they argued that the Court had made it clear that, in a case argued on the basis that the intelligence authorities had in fact been engaging in unlawful surveillance, the principles set out in §§ 34 to 38 of the Court's judgment in *Klass and Others v. Germany*, 6 September 1978, Series A no. 28 did not apply and, instead, the applicant was required to substantiate his claim with evidence sufficient to satisfy the Court that there was a reasonable likelihood that unlawful interception had occurred (citing *Halford v. the United Kingdom*, 25 June 1997, § 57, *Reports* 1997-III; and *Iliya Stefanov v. Bulgaria*, no. 65755/01, § 49, 22 May 2008). In their view, the applicant had not

established a reasonable likelihood of unlawful interception in his case, for four reasons: (i) there was no evidence to support a claim that the applicant's communications were being intercepted; (ii) the Government emphatically denied that any unlawful interception had taken place; (iii) the rejection of the applicant's complaint by the IPT supported this position (see paragraph 20 above); and (iv) the Commissioner's 2001 report also supported this position (see paragraph 65 above).

117. The Government further argued that complaints regarding calls not being put through or hoax calls did not show that there had been any interception in the applicant's case. They pointed out that, under section 2(2) RIPA, preventing calls from being put through and hoax calls were excluded from the definition of interception (see paragraph 30 above). As such, these activities would not fall within the remit of RIPA. The Government further argued that there was no factual foundation for the applicant's claims that any interception was intended to intimidate him.

b. The Court's assessment

118. It is not disputed that mail, telephone and email communications, including those made in the context of business dealings, are covered by the notions of "private life" and "correspondence" in Article 8 § 1.

119. The Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see, *inter alia*, *Klass and Others*, cited above, § 33; *N.C. v. Italy* [GC], no. 24952/94, § 56, ECHR 2002-X; and *Krone Verlag GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01, § 26, 9 November 2006). However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has permitted general challenges to the relevant legislative regime.

120. The Court's approach to assessing whether there has been an interference in cases raising a general complaint about secret surveillance measures was set out in its *Klass and Others* judgment, cited above, §§ 34 to 38 and 41:

> "34. ... The question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious.

The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.

35. In the light of these considerations, it has now to be ascertained whether, by reason of the particular legislation being challenged, the applicants can claim to be victims ... of a violation of Article 8 ... of the Convention ...

36. The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 ... could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 ..., or even to be deprived of the right granted by that Article ..., without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions.

...

The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 ..., since otherwise Article 8 ... runs the risk of being nullified.

37. As to the facts of the particular case, the Court observes that the contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification in the circumstances laid down in the Federal Constitutional Court's judgment ... To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore, as the Delegates rightly pointed out, this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 ...

...

38. Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to '(claim) to be the victim of a violation' of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance ...

...

41. The first matter to be decided is whether and, if so, in what respect the contested legislation, in permitting the above-mentioned measures of surveillance, constitutes an interference with the exercise of the right guaranteed to the applicants under Article 8 para. 1 ....

...

In its report, the Commission expressed the opinion that the secret surveillance provided for under the German legislation amounted to an interference with the

> exercise of the right set forth in Article 8 para. 1 .... Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence."

121. Subsequently, in *Malone v. the United Kingdom*, 2 August 1984, § 64, Series A no. 82, the Court noted:

> "Despite the applicant's allegations, the Government have consistently declined to disclose to what extent, if at all, his telephone calls and mail have been intercepted otherwise on behalf of the police ... They did, however, concede that, as a suspected receiver of stolen goods, he was a member of a class of persons against whom measures of postal and telephone interception were liable to be employed. As the Commission pointed out in its report ..., the existence in England and Wales of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an 'interference ... with the exercise' of the applicant's rights under Article 8 ..., apart from any measures actually taken against him (see the above-mentioned Klass and Others judgment, ibid.). This being so, the Court, like the Commission ..., does not consider it necessary to inquire into the applicant's further claims that both his mail and his telephone calls were intercepted for a number of years."

122. Following *Klass and Others* and *Malone*, the former Commission, in a number of cases against the United Kingdom in which the applicants alleged actual interception of their communications, emphasised that the test in *Klass and Others* could not be interpreted so broadly as to encompass every person in the United Kingdom who feared that the security services may have conducted surveillance of him. Accordingly, the Commission required applicants to demonstrate that there was a "reasonable likelihood" that the measures had been applied to them (see, for example, *Esbester v. the United Kingdom*, no. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, no. 202711/92, Commission decision of 1 September 1993; and *Matthews v. the United Kingdom*, no. 28576/95, Commission decision of 16 October 1996).

123. In cases concerning general complaints about legislation and practice permitting secret surveillance measures, the Court has reiterated the *Klass and Others* approach on a number of occasions (see, *inter alia*, *Weber and Saravia*, cited above, § 78; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 58 to 60, 28 June 2007; *Iliya Stefanov*, cited above, § 49; *Liberty and Others*, cited above, §§ 56 to 57; and *Iordachi and Others v. Moldova*, no. 25198/02, §§ 30 to 35, 10 February 2009). Where actual interception was alleged, the Court has held that in order for there to be an interference, it has to be

satisfied that there was a reasonable likelihood that surveillance measures were applied to the applicant (see *Halford*, cited above, §§ 56 to 57). The Court will make its assessment in light of all the circumstances of the case and will not limit its review to the existence of direct proof that surveillance has taken place given that such proof is generally difficult or impossible to obtain (see *Iliya Stefanov*, cited above, § 50).

124. Sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law *in abstracto*. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court (see *Klass and Others*, cited above, §§ 34 and 36). In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court.

125. The Court observes that the present applicant complained of an interference with his communications both on the basis that, given the circumstances of his particular case, he had established a reasonable likelihood of interception and on the basis of the very existence of measures permitting secret surveillance.

126. The applicant has alleged that the fact that calls were not put through to him and that he received hoax calls demonstrates a reasonable likelihood that his communications are being intercepted. The Court disagrees that such allegations are sufficient to support the applicant's contention that his communications have been intercepted. Accordingly, it concludes that the applicant has failed to demonstrate a reasonable likelihood that there was actual interception in his case.

127. Insofar as the applicant complains about the RIPA regime itself, the Court observes, first, that the RIPA provisions allow any individual who alleges interception of his communications to lodge a complaint with an independent tribunal (see paragraph 75 above), a possibility which was taken up by the applicant. The IPT concluded that no unlawful, within the meaning of RIPA, interception had taken place.

128. As to whether a particular risk of surveillance arises in the applicant's case, the Court notes that under the provisions of RIPA on internal communications, any person within the United Kingdom may have his communications intercepted if interception is deemed necessary on one

or more of the grounds listed in section 5(3) (see paragraphs 31 to 32 above). The applicant has alleged that he is at particular risk of having his communications intercepted as a result of his high-profile murder case, in which he made allegations of police impropriety (see paragraph 5 above), and his subsequent campaigning against miscarriages of justice. The Court observes that neither of these reasons would appear to fall within the grounds listed in section 5(3) RIPA. However, in light of the applicant's allegations that any interception is taking place without lawful basis in order to intimidate him (see paragraph 7 above), the Court considers that it cannot be excluded that secret surveillance measures were applied to him or that he was, at the material time, potentially at risk of being subjected to such measures.

129. In the circumstances, the Court considers that the applicant can complain of an interference with his Article 8 rights. The Government's objection concerning the applicant's lack of victim status is accordingly dismissed.

2. The justification for the interference

130. Any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one of more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim.

a. The parties' submissions

i. The applicant

131. The applicant did not dispute that the surveillance of internal communications in the United Kingdom had a basis in domestic law, namely the provisions of RIPA. Nor did he dispute that both the relevant legislation and the Code were publicly available. However, he argued that the RIPA provisions, and in particular sections 5, 8 and 15 on the issuing of warrants and the relevant safeguards, were not in accordance with the law as required by Article 8 § 2 of the Convention as they did not meet the foreseeability requirement set out in the Court's jurisprudence. In particular, he alleged that section 8(1) RIPA, which stipulated the basic contents of an interception warrant, did not indicate with sufficient clarity how decisions as to which individuals were to be put under surveillance were made; that RIPA did not define the categories of persons who could have their telephones tapped; and that it did not clarify the procedures in place to regulate the interception and processing of intercept material. He contended that the safeguards referred to in section 15 RIPA were inadequate as they were subject to unknown “arrangements” considered necessary by the Secretary of State. The other procedural safeguards in place including the

possibility of launching proceedings before the IPT, were, in the applicant's view, also inadequate to protect against abuse.

132. The applicant relied on the Court's judgment in *Liberty and Others*, cited above, as to the lack of clarity of the relevant provisions of RIPA's predecessor, the Interception of Communications Act 1985, and argued that the changes introduced to the surveillance regime by RIPA were inadequate to address the flaws identified in that case. He concluded that any interference therefore automatically failed to meet the requirement that it must be in accordance with the law and relied in this regard on the conclusions of a report by a surveillance law expert instructed by him, Dr Goold, appended to his submissions. He further highlighted the conclusion of the Court in *Liberty and Others*, cited above, § 68, that the fact that extracts of the code of practice adopted under section 71 RIPA were in the public domain suggested that it was possible for a State to make public certain details about the operation of a scheme for external surveillance without compromising national security.

133. The applicant argued that the Court's decisions in *Valenzuela Contreras v. Spain*, 30 July 1998, *Reports of Judgments and Decisions* 1998-V; *Huvig v. France*, 24 April 1990, Series A no. 176-B; *Kruslin v. France*, 24 April 1990, Series A no. 176-A; *Amann v. Switzerland* [GC], no. 27798/95, ECHR 2000-II; *Al-Nashif v. Bulgaria*, no. 50963/99, 20 June 2002; and *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V had expanded on the issue of "foreseeability" and indicated a departure from the narrower scope of earlier decisions which tolerated the restrictive extent to which national security had imposed blanket secrecy on the publication of surveillance procedures. This broader approach had been confirmed by the Court's recent ruling in *Liberty and Others*, cited above. The applicant argued that the RIPA scheme remained "unnecessarily opaque" and that further details about the operation, beyond those currently included in the Code, should be made available in order to comply with the Convention requirements regarding clarity and precision.

134. As to the safeguards and the arrangements put in place by the Secretary of State under section 15 RIPA, the applicant contended that there was a circularity in the fact that the person responsible for issuing warrants was also responsible for the establishment of the safeguards. He referred to the Court's observation in *Liberty and Others*, cited above, § 66, that details of the arrangements were neither in the legislation nor otherwise in the public domain. As regards the role of the Commissioner, the applicant argued that, as the Court found in *Liberty and Others*, cited above, § 67, the existence of the Commissioner did not contribute towards the accessibility and clarity of the arrangements under section 15 RIPA as he was unable to reveal what the arrangements were.

135. More generally, the applicant alleged that the Government had failed to address properly the safeguards available to prevent abuse of

power. He argued that the legislation failed to identify the nature of the offences which could give rise to an interception order, to define persons liable to have their telephones tapped, to set limits on the duration of telephone tapping and to explain the procedure to be followed in examining and storing data obtained, the precautions to be taken in communicating the data and the circumstances in which data could or should be destroyed (citing *Weber and Saravia*, cited above, § 95).

136. He argued in particular that in *Weber and Saravia*, the law under consideration set out the precise offences the prevention and detection of which could give rise to an interception order, which he alleged was not the case with RIPA. He pointed to the opinion of his expert, Dr Goold, that the definition of "serious crime" in section 81(2)(b) RIPA (see paragraph 34 above) was excessively broad and did not refer to any specific offences by name, and Dr Goold's conclusion that it could not be said that the grounds for issuing a section 8(1) warrant, as set out in section 5(3) RIPA, were sufficiently clear so as to enable an individual to predict what sorts of conduct might give rise to secret surveillance. He further considered that there was no information as to how the categories of persons liable to have their telephones tapped were "strictly controlled", as the Government suggested (see paragraph 142 below).

ii. The Government

137. The Government submitted that any interference which may have arisen in the present case satisfied the requirements of Article 8 § 2. The Government emphasised the duty of democratic governments to uphold the criminal law and protect citizens from terrorist threats and organised crime. In order to discharge this duty, the power to intercept the communications of specific targets was necessary. They pointed to the Commissioner's consistent conclusions that the interception powers under RIPA were an invaluable weapon for the protection of national security and the fight against organised crime (see paragraphs 64 and 72 above). Further, in order for interception to yield useful intelligence, the fact of the interception, as well as the methods by which it could be effected, had to be kept secret. If possible targets were able to gain insight into sensitive interception techniques and capabilities, then they would be able to take steps to undermine the usefulness of any intelligence gathered against them. The Government explained that they had had experience of information about surveillance techniques being put in the public domain, which had led directly to the loss of important sources of intelligence. They insisted that their policy of "neither confirm nor deny" was important to ensure the overall effectiveness of surveillance operations.

138. Generally, regarding the applicant's reliance on the Court's judgment in *Liberty and Others*, cited above, the Government emphasised that that case concerned the Interception of Communications Act 1985, and

not RIPA. Accordingly, they argued, the Court had not given a view as to whether it considered that the provisions of RIPA satisfied the requirements of Article 8. In finding a violation of Article 8 in *Liberty and Others* as a result of the failure of the Government to provide any public indication of the procedure for selecting for examination, sharing, storing and destroying intercepted data, the Court referred specifically at § 68 of its judgment to the fact that under RIPA, the Government had published a code of practice giving details about the operation of the scheme. In the Government's view, the publication of the Code was a feature by which the RIPA scheme could be distinguished from its predecessor in a significant and relevant respect. They also contrasted the finding of the Court in *Liberty and Others*, § 66, as regards the former arrangements regarding safeguards under section 6 Interception of Communications Act with the section 15 RIPA arrangements and the relevant provisions of the Code.

139. On the question whether any interference was in accordance with the law, the Government considered, first, that the statutory provisions of RIPA provided a sufficient basis in domestic law for any interference. They noted that the applicant did not appear to dispute this. As to whether the law was accessible, the Government pointed out that both RIPA and the Code were public accessible. They concluded that the accessibility requirement was satisfied, again noting the absence of any dispute on the matter from the applicant.

140. Regarding foreseeability, the Government highlighted at the outset the special context of secret surveillance. Referring to, *inter alia*, *Weber and Saravia*, cited above, § 93, the Government emphasised that foreseeability could not mean that an individual should be able to foresee when the authorities were likely to intercept his communications so that he could adapt his conduct accordingly. However, they agreed that there needed to be clear, detailed rules on interception, as outlined in § 95 of the Court's judgment in *Weber and Saravia* to guard against the risk of arbitrary exercise of secret surveillance powers. The Court had recently clarified in *Liberty and Others*, cited above, §§ 67 to 69, that not every provision regulating secret surveillance had to be set out in primary legislation. The test was whether there was a sufficient indication of the safeguards in a form accessible to the public in order to avoid abuses of power (citing *Weber and Saravia*, § 95). The Government accordingly contended that account should be taken of all relevant circumstances, including the nature, scope and duration of possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the remedies provided by national law (citing *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, cited above, § 77). They also argued that the Court should consider any evidence as to the actual operation of the warrant system and whether the system appeared to be working properly or was in fact subject to abuse (referring to

Association for European Integration and Human Rights and Ekimdzhiev, §§ 92 to 93).

141. Addressing each of the individual safeguards set out in *Weber and Saravia* in turn, the Government contended, first, as regards the nature of offences which could give rise to an interception order, that section 5(3) RIPA, supplemented by the Code and the relevant definitions provided in the Act, was sufficiently clear and precise in setting out the grounds on which a section 8(1) warrant could be issued. As to the applicant's particular complaint that the term "national security" lacked clarity, the Government emphasised that the term was not criticised by the Court in *Liberty and Others* when it was considered in the context of RIPA's predecessor, a fact which was unsurprising given that the term was a frequently-used legislative concept in the legal systems of many Contracting States and appeared in Article 8 § 2 of the Convention itself. The Government invited the Court to follow the Commission in *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994, in finding that the term "national security" was sufficiently foreseeable for the purposes of Article 8, noting that the applicant had cited no authority to the contrary. The Government also contested the applicant's complaint that "serious crime" was not sufficiently specific and that RIPA failed to clarify the exact offences for the prevention of which a section 8(1) warrant could be issued. They pointed out that nothing in *Weber and Saravia*, cited above, § 27, supported the proposition that the legislative framework had to refer to the relevant offences by name in order to comply with the foreseeability requirement. They concluded that "serious crime", as defined in the Act, provided an adequate indication of the circumstances in which interception could be authorised.

142. Second, as regards the categories of persons liable to have their telephones tapped, the Government acknowledged that RIPA allowed any type of communication transmitted over a telecommunications system to be intercepted. However, the categories of persons liable to have their telephones tapped were strictly controlled by RIPA. The factors by reference to which interception was undertaken had to be specifically identified in the schedule to the warrant. Further, a person would only become a subject of interception, and a set of premises would only be named in an interception warrant, if the interception operation was necessary on one or more of the grounds listed in section 5(3) (see paragraphs 31 to 32 above). The Government disputed that the Court's conclusion in *Weber and Saravia*, cited above, § 97, was at odds with this approach as, in their submission, that judgment merely approved the approach taken in the G10 Act without ruling out other possible methods of satisfying the Article 8 § 2 requirements.

143. Third, RIPA set out strict limits regarding the duration of any interception activity and the circumstances in which a warrant could be renewed (see paragraphs 50 to 51 above).

144. Fourth, RIPA, supplemented by the Code, contained detailed provisions on the procedure to be followed for examining, using and storing the data obtained and the precautions to be taken when communicating the data to other parties. Although in principle an intercepting agency could listen to all intercepted material in order to determine whether it contained valuable intelligence, where it contained no such intelligence the material would be swiftly and securely destroyed. Section 15 RIPA provided an exhaustive definition of the "authorised purposes" and, in particular, section 15(4) identified limits on the number of persons to whom intercept material could be disclosed (see paragraph 42 above). These provisions were supplemented by the provisions of chapter 6 of the Code (see paragraphs 45 to 47 above). In particular, paragraph 6.4 of the Code specified that disclosure could only be made to persons with security clearance and paragraph 6.9 provided for distribution lists of vetted persons to be maintained. Disclosure was further limited by the "need-to-know" principle, which restricted both those who could gain access to intercept material and the extent of any such access. Paragraph 6.5 of the Code clarified that the obligation not to disclose intercept information applied to any person to whom such information had been disclosed. Any breach of these safeguards was an offence under section 19 RIPA (see paragraph 44 above). The requirement to keep records in respect of the making, distribution and destruction of intercept material also provided an important safeguard. Section 15(3) made it clear that intercept material had to be destroyed as soon as there were no longer grounds for retaining it as "necessary" for any of the exhaustively defined authorised purposes. Where human or technical error had resulted in material being gathered where it should not have been, the intercept material was immediately destroyed. Finally, where intercept material was retained, paragraph 6.8 of the Code required it to be reviewed at appropriate intervals to ensure that the justification for its retention remained valid.

145. The Government emphasised that information concerning the arrangements put in place under section 15 RIPA had been published in the Code. However, in order to maintain the operational effectiveness of interception techniques, it was not possible to publish full details of the arrangements. In the view of the Government, the publication of any more detail than had already been published would be contrary to national security and prejudicial to the prevention and detection of serious crime. They argued that the decision as to how much information on safeguards could safely be put in the public domain without undermining the interests of national security or prejudicing the prevention and detection of serious crime fell within their margin of appreciation. It was also significant that the

full details of the arrangements in place were made available to the Commissioner, who was required to keep them under review. The Government emphasised that the Commissioner's approval was sought and given in respect of the safeguard documents either before or shortly after the entry into force of RIPA (see paragraph 63 above). They further emphasised that the Commissioner had expressed his satisfaction with the section 15 safeguards in every report prepared since 2000. They referred in particular to the Commissioner's 2002 and 2004 reports (see paragraphs 68 to 69 above).

146. In conclusion, the Government contended that in light of the detail in the legislation and the applicable code, the RIPA regime satisfied the requirement of lawfulness.

147. The Government also insisted that any interference pursued a legitimate aim. The Government emphatically denied, in this regard, the applicant's allegation that interception was being used to intimidate him and undermine his business activities. The three relevant objectives set out in section 5(3) RIPA, namely safeguarding national security, preventing or detecting serious crime and safeguarding the economic well-being of the United Kingdom, were all legitimate aims for the purposes of Article 8(2).

148. As to proportionality, the Government pointed to the fact that the Court had already accepted that secret surveillance could be necessary in a democratic society (see *Klass and Others*, cited above, § 48) and argued that the surveillance regime in RIPA was necessary and proportionate. The Government further argued that States enjoyed a fairly wide margin of appreciation when legislating in this field (citing *Weber and Saravia*, § 106). They reiterated that the protection of national security in particular was a heavy political responsibility affecting the whole population. Decisions in this area accordingly required a democratic legitimacy which could not be provided by the Court. This had been implicitly recognised by the Court in its *Klass and Others* judgment, cited above, § 49.

149. The Government accepted that in order to demonstrate respect for Article 8(2), there had to be adequate and effective guarantees against abuse of power. They reiterated that the assessment of whether such guarantees were present had to be made in light of all the circumstances of the case. In respect of the surveillance regime applicable in the United Kingdom, the Government emphasised that any interception without lawful authority was a criminal offence under section 1 RIPA (see paragraph 29 above); that the Secretary of State personally issued and modified warrants (see paragraph 38 above); and that guidance was publicly available in the form of the Code. They further pointed to the additional safeguards available in the form of the section 15 safeguards, the oversight of the Commissioner and the jurisdiction of the IPT. They concluded that the RIPA regime contained adequate and effective guarantees against abuse. The involvement of Secretaries of State in the issuing of an interception warrant

provided a real and practical safeguard in the system, as demonstrated by the findings of the Commissioner as to the care and attention they demonstrated in their warrantry work (see paragraphs 62, 67 and 71 above). Further, it was significant that none of the Commissioners' reports referred to any deliberate breach of the RIPA provisions or any unlawful use of interception powers to intimidate a person. Any errors or breaches which had arisen had been the result of technical or human error and had been promptly corrected upon their discovery. As to the jurisdiction of the IPT, the Government emphasised that a challenge could be brought at any time by a person who suspected that his communications were being intercepted. They contrasted this unlimited jurisdiction with the legal regime at issue in *Weber and Saravia* where judicial oversight was limited to cases where an individual had been notified that measures had been taken against him. The applicant in the present case was able to bring his complaint before two senior judges, who ruled that there was no unlawful interception in his case.

150. In conclusion, the Government invited the Court to find that there had been no violation of Article 8 in the present case.

b. The Court's assessment

i. General principles

151. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met where three conditions are satisfied. First, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him (see, among many other authorities, *Rotaru v. Romania*, cited above, § 52; *Liberty and Others*, cited above, § 59; and *Iordachi and Others*, cited above, § 37).

152. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields (see *Malone*, cited above, § 67; *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116; *Association for European Integration*, cited above, § 79; and *Al-Nashif*, cited above, § 121). In its admissibility decision in *Weber and Saravia*, cited above, §§ 93 to 95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field:

> "93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander* [*v. Sweden,* judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia*, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru*). It is therefore essential to have clear, detailed rules on interception of

telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."

153. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106).

154. The Court has acknowledged that the Contracting States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning

of Article 8 § 2, are not to be exceeded (see *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009).

ii. Application of the general principles to the facts of the case

155. The Court recalls that it has found there to be an interference under Article 8 § 1 in respect of the applicant's general complaint about the RIPA provisions and not in respect of any actual interception activity allegedly taking place. Accordingly, in its examination of the justification for the interference under Article 8 § 2, the Court is required to examine the proportionality of the RIPA legislation itself and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicant. In the circumstances, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with in respect of the RIPA regime and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see *Kvasnica*, cited above, § 84). Further, the Court considers it clear that the surveillance measures permitted by RIPA pursue the legitimate aims of the protection of national security, the prevention of crime and the protection of the economic well-being of the country. This was not disputed by the parties.

156. In order to assess whether the RIPA provisions meet the foreseeability requirement, the Court must first examine whether the provisions of the Code can be taken into account insofar as they supplement and further explain the relevant legislative provisions. In this regard, the Court refers to its finding in *Silver and Others v. the United Kingdom*, 25 March 1983, §§ 88 to 89, Series A no. 61 that administrative orders and instructions concerning the scheme for screening prisoners' letters established a practice which had to be followed save in exceptional circumstances and that, as a consequence, although they did not themselves have the force of law, to the extent to which those concerned were made sufficiently aware of their contents they could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the Prison Rules.

157. In the present case, the Court notes, first, that the Code is a public document and is available on the Internet (see paragraphs 26 and 28 above). Prior to its entry into force, it was laid before Parliament and approved by both Houses (see paragraph 26 above). Those exercising duties relating to interception of communications must have regard to its provisions and the provisions of the Code may be taken into account by courts and tribunals (see paragraph 27 above). In light of these considerations, the Court finds that the provisions of the Code can be taken into account in assessing the foreseeability of the RIPA regime.

158. The Court will therefore examine the RIPA regime with reference to each of the safeguards and the guarantees against abuse outlined in *Weber and Saravia* (see paragraphs 152 and 153 above) and, where relevant, to its findings in respect of the previous legislation at issue in *Liberty and Others*, cited above.

159. As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, section 5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom (see paragraphs 31 to 32 above). The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance (*Al-Nashif*, cited above, § 121). Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means (see paragraph 33 above). As for "serious crime", this is defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime is also explained in the Act (see paragraphs 34 to 35 above). The Court is of the view that the reference to serious crime, together with the interpretative clarifications in the Act, gives citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures. The Court therefore considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to an interception order is sufficiently clear (compare and contrast *Iordachi and Others*, cited above, § 46).

160. The Court observes that under RIPA, it is possible for the communications of any person in the United Kingdom to be intercepted. However, it should be recalled that, in contrast to the *Liberty and Others*

case which concerned the legislation on interception of communications between the United Kingdom and any other country, the present case concerns internal communications, i.e. communications within the United Kingdom. Further, the legislation must describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraph, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Finally, the Court notes that in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered (see paragraphs 40 to 41 above). Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA (cf. *Liberty and Others*, cited above, § 64). The Court considers that, in the circumstances, no further clarification in the legislation or the Code of the categories of persons liable to have their communications intercepted can reasonably be required.

161. In respect of the duration of any telephone tapping, the Act clearly stipulates, first, the period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed (see paragraph 50 to 51 above). Although a warrant can be renewed indefinitely, the Secretary of State himself must authorise any renewal and, upon such authorisation, must again satisfy himself that the warrant remains necessary on the grounds stipulated in section 5(3) (see paragraph 51 above). In the context of national security and serious crime, the Court observes that the scale of the criminal activities involved is such that their planning often takes some time. Subsequent investigations may also be of some duration, in light of the general complexity of such cases and the numbers of individuals involved. The Court is therefore of the view that the overall duration of any interception measures will depend on the complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities. The Code explains that the person seeking the renewal must make an application to the Secretary of State providing an update and assessing the value of the interception operation to date. He must specifically address why he considers that the warrant remains necessary on section 5(3) grounds (see paragraph 54 above). Further, under section 9(3) RIPA, the Secretary of State is obliged to cancel a warrant where he is satisfied that the warrant is no longer necessary on

section 5(3) grounds (see paragraph 52 above). There is also provision in the Act for specific factors in the schedule to the warrant to be deleted where the Secretary of State considers that they are no longer relevant for identifying communications from or to the interception subject (see paragraph 53 above). The Code advises that the duty on the Secretary of State to cancel warrants which are no longer necessary means, in practice, that intercepting agencies must keep their warrants under continuous review (see paragraph 55 above). The Court concludes that the provisions on duration, renewal and cancellation are sufficiently clear.

162. As regards the procedure for examining, using and storing the data, the Government indicated in their submissions that, under RIPA, an intercepting agency could, in principle, listen to all intercept material collected (see paragraph 144 above). The Court recalls its conclusion in *Liberty and Others*, cited above, § 65, that the authorities' discretion to capture and listen to captured material was very wide. However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only (cf. *Liberty and Others*, cited above, § 64), thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.

163. As to the general safeguards which apply to the processing and communication of intercept material, the Court observes that section 15 RIPA imposes a duty on the Secretary of State to ensure that arrangements are in place to secure any data obtained from interception and contains specific provisions on communication of intercept material (see paragraph 42 above). Further details of the arrangements are provided by the Code. In particular, the Code strictly limits the number of persons to whom intercept material can be disclosed, imposing a requirement for the appropriate level of security clearance as well as a requirement to communicate data only where there is a "need to know". It further clarifies that only so much of the intercept material as the individual needs to know is to be disclosed and that where a summary of the material would suffice, then only a summary should be disclosed. The Code requires intercept material, as well as copies and summaries of such material, to be handled and stored securely to minimise the risk of threat or loss. In particular, it must be inaccessible to those without the necessary security clearance (see paragraphs 46 to 47 above). A strict procedure for security vetting is in place (see paragraph 48 above). In the circumstances, the Court is satisfied that the provisions on processing and communication of intercept material provide adequate safeguards for the protection of data obtained.

164. As far as the destruction of intercept material is concerned, section 15(3) RIPA requires that the intercept material and any related communications data, as well as any copies made of the material or data, must be destroyed as soon as there are no longer any grounds for retaining them as necessary on section 5(3) grounds (see paragraph 42 above). The Code stipulates that intercept material must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid (see paragraph 55 above).

165. The Code also requires intercepting agencies to keep detailed records of interception warrants for which they have applied (see paragraph 56 above), an obligation which the Court considers is particularly important in the context of the powers and duties of the Commissioner and the IPT (see paragraphs 166 to 167 below)

166. As regards supervision of the RIPA regime, the Court observes that apart from the periodic review of interception warrants and materials by intercepting agencies and, where appropriate, the Secretary of State, the Interception of Communications Commissioner established under RIPA is tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. He has described his role as one of protecting members of the public from unlawful intrusion into their private lives, of assisting the intercepting agencies in their work, of ensuring that proper safeguards are in place to protect the public and of advising the Government and approving the safeguard documents (see paragraph 70 above). The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office (see paragraph 57 above). He reports annually to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes) which is laid before Parliament (see paragraph 61 above). In undertaking his review of surveillance practices, he has access to all relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires (see paragraph 59 above). The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements (see paragraphs 59 and 68 above). The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself.

167. The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such

harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, cited above, § 56). In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems (see, for example, the G 10 Law discussed in the context of *Klass and Others* and *Weber and Saravia*, both cited above), any person who suspects that his communications have been or are being intercepted may apply to the IPT (see paragraph 76 above). The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers (see paragraph 75 above). In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant (see paragraph 78 above). In the event that the IPT finds in the applicant's favour, it can, *inter alia*, quash any interception order, require destruction of intercept material and order compensation to be paid (see paragraph 80 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see paragraph 89 above).

168. Finally, the Court observes that the reports of the Commissioner scrutinise any errors which have occurred in the operation of the legislation. In his 2007 report, the Commissioner commented that none of the breaches or errors identified were deliberate and that, where interception had, as a consequence of human or technical error, unlawfully taken place, any intercept material was destroyed as soon as the error was discovered (see paragraph 73 above). There is therefore no evidence that any deliberate abuse of interception powers is taking place.

169. In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur (see paragraphs 62, 67, 71 and 73 above). Having regard to the safeguards against abuse in the procedures as well as the more general safeguards

offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8 § 2.

170. There has accordingly been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

171. The applicant complained of a violation of his right to a fair hearing in respect of the proceedings before the Investigatory Powers Tribunal. He relied on Article 6 of the Convention, which provides insofar as relevant that:

> "In the determination of his civil rights and obligations ... everyone is entitled to a fair ... hearing ... by [a] ... tribunal ...".

A. Admissibility

172. The Government contested the applicability of Article 6 § 1 to the proceedings in question, arguing that there was no "civil right" in the present case. The Court considers, in light of the parties' submissions, that the complaint raises serious issues of fact and law under the Convention, the determination of which requires an examination of the merits. It therefore concludes that the complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention.. It further notes that it is not inadmissible on any other grounds. The complaint must therefore be declared admissible.

B. Merits

1. The applicability of Article 6 § 1

a. The parties' submissions

173. The applicant alleged that the proceedings before the IPT involved the determination of his civil rights. This was the conclusion reached by the IPT in its ruling on preliminary issues of law, in which it found that Article 6 § 1 was applicable. The applicant referred to the Court's practice whereby, where national courts had conducted a comprehensive and convincing analysis on the basis of relevant Convention case-law and principles, as in the present case, the Court would need very strong reasons to depart from their conclusions and substitute its own views for those of national courts in interpreting domestic law (citing, inter alia, *Masson and Van Zon v. the Netherlands*, 28 September 1995, § 49, Series A no. 327-A;

and *Roche v. the United Kingdom* [GC], no. 32555/96, § 120, ECHR 2005-X). He concluded that the IPT was correct to find that Article 6 § 1 was applicable to the proceedings before it.

174. The Government argued that although the applicant had a right, as a matter of domestic law, to complain to the IPT while the alleged interception was ongoing, the right at issue was not a "civil" right for the purposes of Article 6 § 1 (relying on the Court's judgments in *Klass and Others*, cited above, §§ 57 to 58 and 75; and *Association for European Integration and Human Rights*, cited above, § 106). They contended that, insofar as the use of interception powers remains validly secret, the requirements of Article 6 could not apply to the dispute (referring to *Klass and Others*, cited above, § 75). In the present case, the applicant's position before the IPT was that the interception was continuing. As a result, the Government considered that the validity of the "neither confirm nor deny" stance taken by the authorities could not be impugned. The particular position taken by the Court in interception cases (including *Association for European Integration and Human Rights*) that rights in the field of secret interception powers were not civil rights was, they argued, supported by the Court's general jurisprudence on "civil rights" (citing *Ferrazzini v. Italy* [GC], no. 44759/98, §§ 25, 28 and 30, ECHR 2001-VII; and *Maaouia v. France* [GC], no. 39652/98, § 38, ECHR 2000-X).

175. The Government pointed to the Court's consistent case-law that the concept of "civil rights and obligations" was autonomous and could not be interpreted solely by reference to the domestic law of the respondent State and concluded that the fact that RIPA offered the additional safeguard of an application to the IPT at any time could not in itself make Article 6 § 1 apply to such disputes. As regards the applicant's argument that the Court should be slow to interfere with the ruling of the IPT that Article 6 § 1 was applicable, the Government contested that the question whether Article 6 § 1 was applicable was a matter of domestic law. In their view, *Ferrazzini*, cited above, § 24, was support for the proposition that the applicability of Article 6 § 1 was a matter of Convention law and fell within the competence of the Court.

176. The Government finally noted that the IPT's ruling was issued before the Court's judgment in *Association for European Integration and Human Rights*, cited above, § 106, in which the Court reached the conclusion that Article 6 § 1 did not apply to such proceedings. It was clear that secret powers of interception which were used solely in the interests of national security or in order to prevent and detect serious crime formed part of the "hard core of public authority prerogatives", such that it was inappropriate to classify any related rights and obligations as "civil" in nature (citing *Ferrazzini*, § 29; and *Vilho Eskelinen and Others v. Finland* [GC], no. 63235/00, § 61, ECHR 2007-IV).

b. The Court's assessment

177. The Court in *Klass and Others*, cited above, did not express an opinion on whether Article 6 § 1 applied to proceedings concerning a decision to place a person under surveillance (see § 75 of the Court's judgment). However, the matter was considered by the former Commission in its prior report (*Klass and Others*, no. 5029/71, Report of the Commission, Series B no. 26, pp 35 to 37, §§ 57 to 61). In particular, the Commission noted (§ 58):

> "... Supervisory measures of the kind in question are typical acts of State authority in the public interest and carried out jure imperii. They cannot be questioned before any courts in many legal systems. They do not at all directly concern private rights. The Commission concludes therefore, that [Article] 6 does not apply to this kind of State interference on security grounds."

178. In its recent ruling on the applicability of Article 6 § 1 to proceedings concerning secret surveillance in *Association for European Integration and Human Rights*, cited above, § 106, the Court referred generally to the finding of the Commission in its report in the case of *Klass and Others* that Article 6 § 1 was not applicable in either its civil or criminal limb. In the absence of submissions from the parties on the matter, the Court concluded that nothing in the circumstances of the case before it altered the conclusion in the *Klass and Others* report and that there was therefore no violation of Article 6 § 1.

179. The Court notes that, in the present case, the IPT was satisfied that rights of confidentiality and of privacy for person, property and communications enjoyed a broad level of protection in English private law and that the proceedings before the tribunal therefore involved the determination of "civil rights" within the meaning of Article 6 § 1. The Court recalls that, according to its case-law, the concept of "civil rights and obligations" cannot be interpreted solely by reference to the domestic law of the respondent State. It has on several occasions affirmed the principle that this concept is "autonomous", within the meaning of Article 6 § 1 of the Convention (see *Ferrazzini v. Italy* [GC], no. 44759/98, § 24, ECHR 2001-VII; and *Roche v. the United Kingdom* [GC], no. 32555/96, § 119, ECHR 2005-X). However, in the present case, it is unnecessary to reach a conclusion as to whether Article 6 § 1 applies to proceedings of this nature as, for the reasons outlined below, assuming that Article 6 § 1 applies to the proceedings, the Court considers that the IPT's rules of procedure complied with the requirements of Article 6 § 1.

2. Compliance with Article 6 § 1

a. The parties' submissions

180. The applicant recalled that restrictions on court proceedings could only be compatible with Article 6 § 1 where they pursued a legitimate aim

and there was a reasonable relationship of proportionality between the means employed and the aim sought to be pursued. Further, limitations could not impair the very essence of fair trial rights and any restrictions had to be sufficiently counterbalanced by the procedures followed by the judicial authorities (citing *Rowe and Davis v. the United Kingdom* [GC], no. 28901/95, § 61, ECHR 2000-II). Although the applicant appeared to accept that the restrictions on the procedure before the IPT pursued the legitimate aim of securing that information was not disclosed contrary to the public interest, national security or the detection and prevention of serious crime, he argued that they were not proportionate and impaired the very essence of his right to a fair hearing. In particular, the applicant contended that Rule 6(2) to (5) (restrictions on disclosure and evidence), Rule 9 (secrecy of proceedings) and section 68 RIPA together with Rule 13 (the refusal to provide any reasons to unsuccessful complainants) were contrary to the principle of equality of arms.

181. The applicant submitted that even where national security was at stake, a domestic court could not infringe the fair hearing principle in a blanket and uncritical manner. He argued that less restrictive measures were available to achieve the aim pursued, including arrangements to protect witnesses' identities, disclosure of documents with redactions approved by the IPT, provision of a summary of particularly sensitive material under the supervision of the IPT and appointment of special advocates to whom disclosure of sensitive material could be made. He referred to a recent report on secret evidence published in June 2009 by the non-governmental organisation, JUSTICE, which called for the strengthening of disclosure procedures and increased transparency in court proceedings.

182. The Government emphasised that even where Article 6 § 1 applied to a field falling within the traditional sphere of public law, this did not in itself determine how the various guarantees of Article 6 should be applied to such disputes (citing *Vilho Eskelinen and Others*, cited above, § 64). The obligation to read the Convention as a whole meant that the scope of the Article 6 guarantees in such a case should be in harmony with the Court's approach to judicial control under Article 8. The Government argued that the overarching consideration was that an individual could not be notified of interception measures while interception was ongoing or where notification would jeopardise the capabilities or operations of intercepting agencies. They therefore disputed that the less restrictive measures proposed by the applicant were appropriate. They noted that protection of witnesses' identities would not assist in keeping secret whether interception had occurred. Nor would disclosure of redacted documents or summaries of sensitive material. Further, unless they were appointed in every case, the appointment of special advocates would also allow a complainant to draw inferences about whether his communications had been intercepted.

183. The Government argued that the procedure before the IPT offered as fair a procedure as could be achieved in the context of secret surveillance powers. In particular, a complainant did not have to overcome any evidential burden to apply to the IPT and any legal issues could be determined in a public judgment after an *inter partes* hearing. Further, the IPT had full powers to obtain any material it considered necessary from relevant bodies and could call upon the assistance of the Commissioner. It could appoint an advocate to assist it at closed hearings. Finally, in the event that the complainant was successful, a reasoned decision would be provided. The Government accordingly disputed that the very essence of the applicant's right to a fair trial had been impaired.

b. The Court's assessment

184. The Court reiterates that according to the principle of equality of arms, as one of the features of the wider concept of a fair trial, each party must be afforded a reasonable opportunity to present his case under conditions that do not place him at a substantial disadvantage *vis-à-vis* his opponent (see, for example, *Jespers v. Belgium*, no. 8403/78, Commission decision of 15 October 1980, Decisions and Reports (DR) 27, p. 61; *Foucher v. France*, judgment of 18 March 1997, *Reports* 1997-II, § 34; and *Bulut v. Austria*, judgment of 22 February 1996, *Reports* 1996-II, p. 380-81, § 47). The Court has held nonetheless that, even in proceedings under Article 6 for the determination of guilt on criminal charges, there may be restrictions on the right to a fully adversarial procedure where strictly necessary in the light of a strong countervailing public interest, such as national security, the need to keep secret certain police methods of investigation or the protection of the fundamental rights of another person. There will not be a fair trial, however, unless any difficulties caused to the defendant by a limitation on his rights are sufficiently counterbalanced by the procedures followed by the judicial authorities (see, for example, *Doorson v. the Netherlands*, judgment of 26 March 1996, § 70, *Reports* 1996-II; *Jasper v. the United Kingdom* [GC], no. 27052/95, §§ 51 to 53, ECHR 2000-II; and *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 205, ECHR 2009-....). A similar approach applies in the context of civil proceedings.

185. The Court notes that the IPT, in its preliminary ruling of 23 January 2003, considered the applicant's complaints regarding the compliance of the Rules with Article 6 § 1. It found that, with the exception of Rule 9(6) which required all oral hearings to be held in private, the Rules challenged by the applicant were proportionate and necessary, with special regard to the need to preserve the Government's "neither confirm nor deny policy" (see paragraphs 92 to 95 above).

186. At the outset, the Court emphasises that the proceedings related to secret surveillance measures and that there was therefore a need to keep

secret sensitive and confidential information. In the Court's view, this consideration justifies restrictions in the IPT proceedings. The question is whether the restrictions, taken as a whole, were disproportionate or impaired the very essence of the applicant's right to a fair trial.

187. In respect of the rules limiting disclosure, the Court recalls that the entitlement to disclosure of relevant evidence is not an absolute right. The interests of national security or the need to keep secret methods of investigation of crime must be weighed against the general right to adversarial proceedings (see, *mutatis mutandis*, *Edwards and Lewis v. the United Kingdom* [GC], nos. 39647/98 and 40461/98, § 46, ECHR 2004-X). The Court notes that the prohibition on disclosure set out in Rule 6(2) admits of exceptions, set out in Rules 6(3) and (4). Accordingly, the prohibition is not an absolute one. The Court further observes that documents submitted to the IPT in respect of a specific complaint, as well as details of any witnesses who have provided evidence, are likely to be highly sensitive, particularly when viewed in light of the Government's "neither confirm nor deny" policy. The Court agrees with the Government that, in the circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place. It is also relevant that where the IPT finds in the applicant's favour, it can exercise its discretion to disclose such documents and information under Rule 6(4) (see paragraph 84 above).

188. As regards limitations on oral and public hearings, the Court recalls, first, that the obligation to hold a hearing is not absolute. There may be proceedings in which an oral hearing is not required and where the courts may fairly and reasonably decide the case on the basis of the parties' submissions and other written materials. The character of the circumstances that may justify dispensing with an oral hearing essentially comes down to the nature of the issues to be decided by the competent national court (see *Jussila v. Finland* [GC], no. 73053/01, §§ 41 to 42, ECHR 2006-XIII). The Court notes that Rule 9(2) provides that oral hearings are within the IPT's discretion and it is clear that there is nothing to prevent the IPT from holding an oral hearing where it considers that such a hearing would assist its examination of the case. As the IPT held in its preliminary ruling, its discretion to hold oral hearings extends to *inter partes* oral hearings, where such hearings can take place without breaching the IPT's duty to prevent the potentially harmful disclosure of sensitive information (see paragraph 92 above). Finally, in respect of the stipulation in Rule 9(6) that hearings must be held in private (interpreted by the IPT not to apply to cases involving the determination of preliminary issues of law – see paragraph 93 above), the Court notes that it is clear from the terms of Article 6 § 1 itself that national security may justify the exclusion of the public from the proceedings.

189. Concerning the provision of reasons, the Court emphasises that the extent to which the duty to give reasons applies may vary according to the nature of the decision and must be determined in the light of the circumstances of the case (see *Ruiz Torija v. Spain*, 9 December 1994, § 29, Series A no. 303-A). In the context of the IPT's proceedings, the Court considers that the "neither confirm nor deny" policy of the Government could be circumvented if an application to the IPT resulted in a complainant being advised whether interception had taken place. In the circumstances, it is sufficient that an applicant be advised that no determination has been in his favour. The Court further notes in this regard that, in the event that a complaint is successful, the complainant is entitled to have information regarding the findings of fact in his case (see paragraph 87 above).

190. In light of the above considerations, the Court considers that the restrictions on the procedure before the IPT did not violate the applicant's right to a fair trial. In reaching this conclusion, the Court emphasises the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT. In order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime, the Court considers that the restrictions on the applicant's rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant's Article 6 rights.

191. Accordingly, assuming that Article 6 § 1 applies to the proceedings in question, there has been no violation of that Article.

III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

192. The applicant further complained that he had no effective remedy in respect of the alleged violation of Articles 6 § 1 and 8 of the Convention. He relied on Article 13 of the Convention, which provides insofar as relevant as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

A. Admissibility

193. The Court notes that the complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

194. The applicant maintained that he had an "arguable claim" under Articles 6 § 1 and 8, and that the proceedings before the IPT did not afford him a remedy as required by Article 13 of the Convention as it did not comply with the requirements of Article 6 § 1.

195. The Government contended that there was no violation of Article 13 in the present case. In particular, they argued that the applicant had no arguable claim to be a victim of a violation of Article 6 § 1 or Article 8; that insofar as the applicant's complaints were in essence ones that challenged the relevant legislative scheme, the Article 13 complaint must fail (citing *Leander v. Sweden*, 26 March 1987, § 77(d), Series A no. 116); and that in any event the IPT offered an effective remedy.

2. The Court's assessment

196. Having regard to its conclusions in respect of Article 8 and Article 6 § 1 above, the Court considers that the IPT offered to the applicant an effective remedy insofar as his complaint was directed towards the alleged interception of his communications.

197. In respect of the applicant's general complaint under Article 8, the Court reiterates its case-law to the effect that Article 13 does not require the law to provide an effective remedy where the alleged violation arises from primary legislation (see *James and Others v. the United Kingdom*, 21 February 1986, § 85, Series A no. 98; and *Leander*, cited above, § 77(d)).

198. There has accordingly been no violation of Article 13.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Joins* to the merits the Government's objection regarding the applicant's lack of victim status and declares the application admissible;

2. *Holds* that there has been no violation of Article 8 of the Convention and *dismisses* in consequence the Government's above-mentioned objection;

3. *Holds* that there has been no violation of Article 6 § 1 of the Convention;

4. *Holds* that there has been no violation of Article 13 of the Convention.

Done in English, and notified in writing on 18 May 2010, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early Registrar	Lech Garlicki President