FOURTH SECTION

CASE OF LIBERTY AND OTHERS
v. THE UNITED KINGDOM

(Application no. 58243/00)

JUDGMENT

STRASBOURG

1 July 2008

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Liberty and Others v. the United Kingdom,

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

Lech Garlicki, *President,*
Nicolas Bratza,
Ljiljana Mijović,
David Thór Björgvinsson,
Ján Šikuta,
Päivi Hirvelä,
Mihai Poalelungi, *judges,*
and Lawrence Early, *Section Registrar*,

Having deliberated in private on 10 June 2008,

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

PROCEDURE

1. The case originated in an application (no. 58243/00) 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 Liberty, British Irish Rights Watch and the Irish Council for Civil

Liberties, a British and two Irish civil liberties' organisations based in London and Dublin respectively, on 9 September 1999.

2. The applicants were represented by Mr A. Gask, a lawyer practising in London. The United Kingdom Government ("the Government") were represented by their Agent, Mr D. Walton, Foreign and Commonwealth Office.

3. On 25 June 2002 the Court decided to communicate the application to the Government, and several rounds of observations were received from the parties. On 22 March 2005 the Court adjourned the case until linked proceedings before the Investigatory Powers Tribunal had concluded (see paragraphs 11-15 below). On 27 February 2006 the Court resumed its examination and, under the provisions of Article 29 § 3 of the Convention, decided to examine the merits of the application at the same time as its admissibility. Further observations were, therefore, sought from the parties.

4. The applicants requested a hearing but the Court decided that it would not be necessary.

THE FACTS

THE CIRCUMSTANCES OF THE CASE

1. The alleged interception of communications

5. The applicants alleged that in the 1990s the Ministry of Defence operated an Electronic Test Facility ("ETF") at Capenhurst, Cheshire, which was built to intercept 10,000 simultaneous telephone channels coming from Dublin to London and on to the continent. Between 1990 and 1997 the applicants claimed that the ETF intercepted all public telecommunications, including telephone, facsimile and e-mail communications, carried on microwave radio between the two British Telecom's radio stations (at Clwyd and Chester), a link which also carried much of Ireland's telecommunications traffic. During this period the applicant organisations were in regular telephone contact with each other and also providing, *inter alia,* legal advice to those who sought their assistance. They alleged that many of their communications would have passed between the British Telecom radio stations referred to above and would thus have been intercepted by the ETF.

2. Complaint to the Interception of Communications Tribunal ("ICT")

6. On 9 September 1999, having seen a television report on the alleged activities of the ETF, the applicant organisations requested the Interception of Communications Tribunal ("the ICT": see paragraphs 28-30 below) to investigate the lawfulness of any warrants which had been issued in respect of the applicants' communications between England and Wales and Ireland. On 19 October 1999 an official of the ICT confirmed that an investigation would proceed and added:

> "... I am directed to advise you that the Tribunal has no way of knowing in advance of an investigation whether a warrant exists in any given case. The Tribunal investigates all complaints in accordance with section 7 of the [Interception of Communications Act 1985: 'the 1985 Act', see paragraphs 16-33 below] establishing whether a relevant warrant or relevant certificate exists or had

existed and, if so, whether there has been any contravention of sections 2 to 5. If ... the Tribunal concludes that there has been a contravention of sections 2 to 5, the Tribunal may take steps under sections 7(4), (5) and (6). In any case where there is found to have been no contravention, the Tribunal is not empowered to disclose whether or not authorised interception has taken place. In such instances, complainants are advised only that there has been no contravention of sections 2 to 5 in relation to a relevant warrant or a relevant certificate."

7. By a letter dated 16 December 1999 the ICT confirmed that it had thoroughly investigated the matter and was satisfied that there had been no contravention of sections 2 to 5 of the 1985 Act in relation to the relevant warrant or certificate.

3. Complaint to the Director of Public Prosecutions ("DPP")

8. By a letter dated 9 September the applicants complained to the DPP of an unlawful interception, requesting the prosecution of those responsible. The DPP passed the matter to the Metropolitan Police for investigation. By a letter dated 7 October 1999 the police explained that no investigation could be completed until the ICT had investigated and that a police investigation might then follow if it could be shown that an unwarranted interception had taken place or if any of the other conditions set out in section 1(2)-(4) of the 1985 Act had not been met. The applicants pointed out, in their letter of 12 October 1999, that the vague, albeit statutory, response of the ICT would mean that they would not know whether a warrant had been issued or, if it had, whether it had been complied with. They would not, therefore, be in a position to make submissions to the police after the ICT investigation as to whether or not a criminal investigation was warranted. The applicants asked if, and if so how, the police could establish for themselves whether or not a warrant had been issued, so as to decide whether an investigation was required, and how the police would investigate, assuming there had been no warrant.

9. The DPP responded on 19 October 1999 that the police had to await the ICT decision, and the police responded on 9 November 1999 that the applicants' concerns were receiving the fullest attention, but that they were unable to enter into discussion on matters of internal procedure and inter-departmental investigation.

10. On 21 December 1999 the applicants wrote to the police pointing out that, having received the decision of the ICT, they still did not know whether or not there had been a warrant or whether there had been unlawful interception. The response, dated 17 January 2000, assured the applicants that police officers were making enquires with the relevant agencies with a view to establishing whether there had been a breach of section 1 of the 1985 Act and identifying the appropriate investigative authority. The police informed the applicants by a letter dated 31 March 2000 that their enquiries continued, and, by a letter dated 13 April 2000, that these enquiries had not revealed an offence contrary to section 1 of the 1985 Act.

4. Complaint to the Investigatory Powers Tribunal ("IPT")

11. On 15 December 2000 the former statutory regime for the interception of communications was replaced by the Regulation of Investigatory Powers Act 2000 (see paragraphs 34-39 below) and a new tribunal, the IPT, was created.

12. On 13 August 2001 the applicants began proceedings in the IPT against the security and intelligence agencies of the United Kingdom, complaining of interferences with their rights to privacy for their telephone and other communications from 2 October

2000 onwards (*British-Irish Rights Watch and others v. The Security Service and others*, IPT/01/62/CH). The IPT, sitting as its President and Vice-President (a Court of Appeal and a High Court judge), had security clearance and was able to proceed in the light not just of open evidence filed by the defendant services but also confidential evidence, which could not be made public for reasons of national security.

13. On 9 December 2004 the IPT made a number of preliminary rulings on points of law. Although the applicants had initially formulated a number of claims, by the time of the ruling these had been narrowed down to a single complaint about the lawfulness of the "filtering process", whereby communications between the United Kingdom and an external source, captured under a warrant pursuant to section 8(4) of the 2000 Act (which had replaced section 3(2) of the 1985 Act: see paragraphs 34-39 below), were sorted and accessed pursuant to secret selection criteria. The question was, therefore, whether "the process of filtering intercepted telephone calls made from the UK to overseas telephones ... breaches Article 8 § 2 [of the Convention] because it is not 'in accordance with the law'".

14. The IPT found that the difference between the warrant schemes for interception of internal and external communications was justifiable, because it was more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, given the substantial potential control it exercised in this field; and also because its knowledge of, and control over, external communications was likely to be much less extensive.

15. As to whether the law was sufficiently accessible and foreseeable for the purposes of Article 8 § 2, the IPT observed:

> "The selection criteria in relation to accessing a large quantity of as yet unexamined material obtained pursuant to a s8(4) warrant (as indeed in relation to material obtained in relation to a s8(1) warrant) are those set out in s5(3) . The Complainants' Counsel complains that there is no 'publicly stated material indicating that a relevant person is satisfied that the [accessing] of a particular individual's telephone call is proportionate'. But the Respondents submit that there is indeed such publicly stated material, namely the provisions of s6(l) of the Human Rights Act which requires a public authority to act compatibly with Convention rights, and thus, it is submitted, imposes a duty to act proportionately in applying to the material the s5(3) criteria.
>
> To that duty there is added the existence of seven safeguards listed by the Respondents' Counsel, namely (1) the criminal prohibition on unlawful interception (2) the involvement of the Secretary of State (3) the guiding role of the Joint Intelligence Committee ('JIC') (4) the Code of Practice (5) the oversight by the Interception of Communication Commissioner (whose powers are set out in Part IV of the Act) (6) the availability of proceedings before this Tribunal and (7) the oversight by the Intelligence and Security Committee, an all-party body of nine Parliamentarians created by the Intelligence Services Act 1994 ...
>
> It is plain that, although in fact the existence of all these safeguards is publicly known, it is not part of the requirements for accessibility or foreseeability that the precise details of those safeguards should be published. The Complainants' Counsel has pointed out that it appears from the Respondents' evidence that there are in existence additional operating procedures, as would be expected given the requirements that there be the extra safeguards required by s16 of the Act, and the obligation of the Secretary of State to ensure their existence under s15(1)(b). It is not suggested by the Complainants that the nature of those operating procedures be disclosed, but that their existence, i.e. something along the lines of what is in the Respondents' evidence, should itself be disclosed in the Code of Practice.
>
> We are unpersuaded by this. First, such a statement in the Code of Practice, namely as to the existence of such procedures, would in fact take the matter no further than it already stands by virtue

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

... [F]oreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security ... In this case the legislation is adequate and the guidelines are clear. Foreseeability does not require that a person who telephones abroad knows that his conversation is going to be intercepted because of the existence of a valid s. 8(4) warrant. ...

The provisions, in this case the right to intercept and access material covered by a s.8(4) warrant, and the criteria by reference to which it is exercised, are in our judgment sufficiently accessible and foreseeable to be in accordance with law. The parameters in which the discretion to conduct interception is carried on, by reference to s. 5(3) and subject to the safeguards referred to, are plain from the face of the statute. In this difficult and perilous area of national security, taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed upon the Respondent, we are satisfied that the balance is properly struck."

B. Relevant domestic law and practice

1. The Interception of Communications Act 1985

16. During the period at issue in this application the relevant legislation was sections 1-10 of the Interception of Communications Act 1985 ("the 1985 Act"), which came into force on 10 April 1986 and was repealed by the Regulation of Investigatory Powers Act 2000 ("the 2000 Act").

17. Pursuant to section 1 of the 1985 Act, a person who intentionally intercepted a communication in the course of its transmission by post or by means of a public telecommunications system was guilty of an offence. A number of exceptions were made, the relevant one being a communication intercepted pursuant to a warrant issued by the Secretary of State under section 2 of the 1985 Act and in accordance with a certificate issued under section 3(2)(b) of the 1985 Act.

(a) Warrants for interception

(i) The three grounds for issuing a warrant

18. The Secretary of State's power to issue a warrant under section 2 of the 1985 Act could be exercised only if he considered the warrant 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."

19. The term "serious crime" was defined by section 10(3) of the Act as follows:

"For the purposes of [the 1985 Act], conduct which constitutes or, if it took place in the United Kingdom, would constitute one or more offences shall be regarded as a serious crime if, and only if –

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

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

20. The scope of the term "national security" was clarified by the Commissioner appointed under the 1985 Act. In his 1986 report he stated (§ 27) 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".

21. In determining whether a warrant was necessary for one of the three reasons set out in section 2(2) of the 1985 Act, the Secretary of State was under a duty to take into account whether the information which it was considered necessary to acquire could reasonably be acquired by other means (section 2(3)). In addition, warrants to safeguard the economic well-being of the United Kingdom could not be issued unless the information to be acquired related to the acts or intentions of persons outside the British Islands (section 2(4)). A warrant required the person to whom it was addressed to intercept, in the course of their transmission by post or by means of a public telecommunications system, such communications as were described in the warrant.

(ii) The two types of warrant

22. Two types of warrant were permitted by section 3 of the 1985 Act. The first, a "section 3(1) warrant", was a warrant that required the interception of:

> "(a) such communications as are sent to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from–
> (i) one particular person specified or described in the warrant; or
> (ii) one particular set of premises so specified or described; and
>
> (b) such other communications (if any) as it is necessary to intercept in order to intercept communications falling within paragraph (a) above."

By section 10(1) of the 1985 Act, the word "person" was defined to include any organisation or combination of persons and the word "address" was defined to mean any postal or telecommunications address.

23. The second type of warrant, a "section 3(2) warrant", was one that required the interception, in the course of transmission by means of a public telecommunications system, of:

> "(i) such external communications as are described in the warrant; and
>
> (ii) such other communications (if any) as it is necessary to intercept in order to intercept such external communications as are so described ...".

24. When he issued a section 3(2) warrant, the Secretary of State was required to issue also a certificate containing a description of the intercepted material the examination of which he considered necessary in the interests of national security, to prevent or detect serious crime or to safeguard the State's economic well-being (section 3(2)(b)). A section 3(2) warrant could not specify an address in the British Islands for the purpose of including communications sent to or from that address in the certified material unless-

> "3(3) (a) the Secretary of State considers that the examination of communications sent to or from that address is necessary for the purpose of preventing or detecting acts of terrorism; and
>
> (b) communications sent to or from that address are included in the certified material only in so far as they are sent within such a period, not exceeding three months, as is specified in the certificate."

25. Section 3(2) warrants could be issued only under the hand of the Secretary of State or a permitted official of high rank with the written authorisation of the Secretary of

State. If issued under the hand of the Secretary of State, the warrant was valid for two months; if by another official, it was valid for two days. Only the Secretary of State could renew a warrant. If the Secretary of State considered that a warrant was no longer necessary in the interests of national security, to prevent or detect serious crime or to safeguard the State's economic well-being, he was under a duty to cancel it (section 4).

26. The annual report of the Commissioner for 1986 explained the difference between warrants issued under section 3(1) and under section 3(2):

> "There are a number of differences ... But the essential differences may be summarised as follows:
>
> (i) Section 3(2) warrants apply only to external telecommunications;
>
> (ii) whereas section 3(1) warrants only apply to communications to or from one particular person ... or one particular set of premises, Section 3(2) warrants are not so confined; but
>
> (iii) at the time of issuing a Section 3(2) warrant the Secretary of State is obliged to issue a certificate describing the material which it is desired to intercept; and which he regards as necessary to examine for any of the purposes set out in Section 2(2).
>
> So the authority to intercept granted by the Secretary of State under Section 3(2) is limited not so much by reference to the target, as it is under section 3(1), but by reference to the material. It follows that in relation to Section 3(2) warrants, I have had to consider first, whether the warrant applies to external communications only, and, secondly, whether the certified material satisfies the Section 2(2) criteria. ...
>
> There is a further important limitation on Section 3(2) warrants. I have said that the authority granted by the Secretary of State is limited by reference to the material specified in the certificate, rather than the targets named in the warrants. This distinction is further underlined by Section 3(3) which provides that material specified shall *not* include the address in the British Islands for the purpose of including communications sent to or from that address, except in the case of counter-terrorism. So if, for example in a case of subversion the Security Service wishes to intercept external communications to or from a resident of the British Islands, he could not do so under a Section 3(2) warrant by asking for communications sent to or from his address to be included in the certified material. But it would be possible for the Security Service to get indirectly, through a legitimate examination of certified material, what it may not get directly. In such cases it has become the practice to apply for a separate warrant under Section 3(1) known as an overlapping warrant, in addition to the warrant under Section 3(2). There is nothing in the [1985 Act] which requires this to be done. But it is obviously a sound practice, and wholly consistent with the legislative intention underlying Section 3(3). Accordingly I would recommend that where it is desired to intercept communications to or from an individual residing in the British Islands, as a separate target, then in all cases other than counter-terrorism there should be a separate warrant under Section 3(1), even though the communications may already be covered by a warrant under Section 3(3). The point is not without practical importance. For the definition of "relevant warrant" and "relevant certificate" in Section 7(9) of the Act makes it clear that, while the Tribunal has power to investigate warrants issued under section 3(1) and certificates under section 3(2) where an address is specified in the certificate, it has no such power to investigate Section 3(2) warrants, where an address is not so certified."

(iii) Use and retention of information

27. Section 6 of the 1985 Act was entitled "Safeguards" and read as follows:

> "(1) Where the Secretary of State issues a warrant he shall, unless such arrangements have already been made, make such arrangements as he considers necessary for the purpose of securing-
>
> (a) that the requirements of subsections (2) and (3) below are satisfied in relation to the intercepted material; and
>
> (b) where a certificate is issued in relation to the warrant, that so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person.

(2) The requirements of this subsection are satisfied in relation to any intercepted material if each of the following, namely-

(a) the extent to which the material is disclosed;

(b) the number of persons to whom any of the material is disclosed;

(c) the extent to which the material is copied; and

(d) the number of copies made of any of the material;

is limited to the minimum that is necessary as mentioned in section 2 (2) above.

(3) The requirements of this subsection are satisfied in relation to any intercepted material if each copy made of any of that material is destroyed as soon as its retention is no longer necessary as mentioned in section 2 (2) above."

(b) The Interception of Communications Tribunal ("ICT")

28. Section 7 of the 1985 Act provided for a Tribunal to investigate complaints from any person who believed that communications sent by or to him had been intercepted. Its jurisdiction, so far as material, was limited to investigating whether there was or had been a "relevant warrant" or a "relevant certificate" and, where there was or had been, whether there had been any contravention of sections 2-5 of the 1985 Act in relation to that warrant or certificate. Section 7(9) read, in so far as relevant, as follows:

"For the purposes of this section –

(a) a warrant is a relevant warrant in relation to an applicant if –

(i) the applicant is specified or described in the warrant; or

(ii) an address used for the transmission of communications to or from a set of premises in the British Islands where the applicant resides or works is so specified;

(b) a certificate is a relevant certificate in relation to an applicant if and to the extent that an address used as mentioned in paragraph (a)(ii) above is specified in the certificate for the purpose of including communications sent to or from that address in the certified material."

29. The ICT applied the principles applicable by a court on an application for judicial review. If it found there had been a contravention of the provisions of the Act, it was to give notice of that finding to the applicant, make a report to the Prime Minister and to the Commissioner appointed under the Act and, where it thought fit, make an order quashing the relevant warrant, directing the destruction of the material intercepted and/or directing the Secretary of State to pay compensation. In other cases, the ICT was to give notice to the applicant stating that there had been no contravention of sections 2-5 of the Act.

30. The ICT consisted of five members, each of whom was required to be a qualified lawyer of not less than ten years standing. They held office for a five-year period and could be re-appointed. The decisions of the ICT were not subject to appeal.

(c) The Commissioner

31. Section 8 provided that a Commissioner be appointed by the Prime Minister. He or she was required to be a person who held, or who had held, high judicial office. The Commissioner's functions included the following:

– to keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 2-5 of the 1985 Act;

– to give to the ICT all such assistance as it might require for the purpose of enabling it to carry out its functions;

– to keep under review the adequacy of the arrangements made under section 6 for safeguarding intercepted material and destroying it where its retention was no longer necessary;

– to report to the Prime Minister if there appeared to have been a contravention of sections 2-5 which had not been reported by the ICT or if the arrangements under section 6 were inadequate;

– to make an annual report to the Prime Minister on the exercise of the Commissioner's functions. This report had to be laid before the Houses of Parliament. The Prime Minister had the power to exclude any matter from the report if publication would have been prejudicial to national security, to the prevention or detection of serious crime or to the well-being of the United Kingdom. The report had to state if any matter had been so excluded.

32. In his first report as Commissioner, in 1992, Sir Thomas Bingham MR, as he then was, explained his own role as part of the safeguards inherent in the 1985 Act as follows:

> "The third major safeguard is provided by the Commissioner himself. While there is nothing to prevent consultation of the Commissioner before a warrant is issued, it is not the practice to consult him in advance and such consultation on a routine basis would not be practicable. So the Commissioner's view is largely retrospective, to check that warrants have not been issued in contravention of the Act and that appropriate procedures were followed. To that end, I have visited all the warrant issuing departments and agencies named in this report, in most cases more than once, and discussed at some length the background to the warrant applications. I have also discussed the procedure for seeking warrants with officials at various levels in all the initiating bodies and presenting departments. I have inspected a significant number of warrants, some chosen by me at random, some put before me because it was felt that I should see them. Although I have described ... a number of instances in which mistakes were made or mishaps occurred, I have seen no case in which the statutory restrictions were deliberately evaded or corners knowingly cut. A salutary practice has grown up by which the Commissioner's attention is specifically drawn to any case in which an error or contravention of the Act has occurred: I accordingly believe that there has been no such case during 1992 of which I am unaware."

Similar conclusions about the authorities' compliance with the law were drawn by all the Commissioners in their reports during the 1990s.

33. In each of the annual reports made under the 1985 Act the Commissioner stated that in his view the arrangements made under section 6 of the 1985 were adequate and complied with, without revealing what the arrangements were. In the 1989 Report the Commissioner noted at § 9 that there had been technological advances in the telecommunications field which had "necessitated the making of further arrangements by the Secretary of State for the safeguarding of material under section 6 of the [1985 Act]". The Commissioner stated that he had reviewed the adequacy of the new arrangements. For the year 1990, the Commissioner recorded that, as a result of a new practice of the police disclosing some material to the Security Service, a further change in the section 6 arrangements had been required. The Commissioner said in the 1990 Report that he was "satisfied with the adequacy of the new arrangements" (1990 Report at § 18). In the 1991 Report, the Commissioner stated that there had been some minor changes to the section 6 arrangements and confirmed that he was satisfied with the arrangements as modified (§ 29 of the 1991 Report). In the 1993 Report, the Commissioner said at § 11:

> "Some of the written statements of section 6 safeguards which I inspected required to be updated to take account of changes in the public telecommunications market since they had been drafted and approved. Other statements could, as it seemed to me, be improved by more explicit rules governing the circumstances and manner in which, and the extent to which, intercept material could be copied. It also seemed to me that it would be advantageous, where this was not already done, to remind all involved m handling intercept material on a regular basis of the safeguards to which they were subject, securing written acknowledgements that the safeguards had been read and understood. These suggestions appeared to be readily accepted by the bodies concerned. They did not in my view indicate any failure to comply with section 6 of the Act."

In his first year as Commissioner, Lord Nolan reported the following on this issue of section 6 safeguards (1994 Report, § 6):

> "Like my predecessors, I have on each of my visits considered and discussed the arrangements made by the Secretary of State under section 6 for the purpose of limiting the dissemination and retention of intercepted material to what is necessary within the meaning of section 2. Each agency has its own set of such arrangements, and there are understandable variations between them. For example, the practical considerations involved in deciding what is necessary in the interests of national security, or the economic well-being of the United Kingdom (the areas with which the Security Service and the Secret Intelligence Service are almost exclusively concerned) are somewhat different from those involved in the prevention and detection of serious criminal offences (with which the police forces and HM Customs & Excise are almost exclusively concerned). I am satisfied that all of the agendas are operating within the existing approved safeguards under the terms of the arrangements as they stand ..."

2. The Regulation of Investigatory Powers Act 2000

34. The 2000 Act came into force on 15 December 2000. The explanatory memorandum described the main purpose of the Act as being to ensure that the relevant investigatory powers were used in accordance with human rights. As to the first, interceptions of communications, the 2000 Act repealed, *inter alia*, sections 1-10 of the 1985 Act and provides for a new regime for the interception of communications.

35. The 2000 Act is designed to cover the purposes for which the relevant investigatory powers may be used, which authorities can use the powers, who should authorise each use of the power, the use that can be made of the material gained, judicial oversight and a means of redress for the individual.

36. A new Investigatory Powers Tribunal ("IPT") assumed the responsibilities of the former ICT, of the Security Services Tribunal and of the Intelligence Services Tribunal. The Interception of Communications Commissioner continues to review the actions of the Secretary of State as regards warrants and certificates and to review the adequacy of the arrangements made for the execution of those warrants. He is also, as before, to assist the Tribunal. In addition, the Secretary of State is to consult about and to publish codes of practice relating to the exercise and performance of duties in relation to, *inter alia*, interceptions of communications.

37. Section 2(2) of the 2000 Act 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 telecommunications 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 of all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."

38. Section 5(2) of the 2000 Act provides that the Secretary of State shall not issue an interception warrant unless he believes that the warrant is necessary, *inter alia*, in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

39. In addition to the general safeguards specified in section 15 of the Act, section 16 provides additional safeguards in the case of certificated warrants (namely warrants for interception of external communications supported by a certificate). In particular, section 16(1) provides that intercepted material is to be read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary for one of the above purposes and falls within subsection (2). Intercepted material falls within subsection (2) so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which is referable to an individual who is known to be for the time being in the British Isles and has as its purpose, or one of its purposes, the identification of material in communications sent by that person, or intended for him.

40. In its Ruling of 9 December 2004 (see paragraphs 13-15 above), the IPT set out the following extracts from the Interception of Communications Code of Practice issued pursuant to s. 71 of the 2000 Act ("the Code of Practice"). Subparagraph 4(2) of the Code of Practice deals with the application for a s. 8(1) warrant as follows :

"An application for a warrant is made to the Secretary of State . . . Each application, a copy of which must be retained by the applicant, should contain the following information :

• Background to the operation in question.

• Person or premises to which the application relates (and how the person or premises feature in the operation) .

• Description of the communications to be intercepted, details of communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.

• Description of the conduct to be authorised as considered necessary in order to carry out the interception, where appropriate.

• An explanation of why the interception is considered to be necessary under the provisions of section 5(3).

• A consideration of why the conduct is to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

• A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.

• Where an application is urgent, supporting justification should be provided.

• An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of the Act .

The IPT continued:

"Applications for a s. 8(4) warrant are addressed in subparagraph 5 .2 of the Code of Practice :

'An application for a warrant is made to the Secretary of State ... each application, a copy of which must be retained by the applicant, should contain the following information :

• Background to the operation in question [identical to the first bullet point in 4.2].

• Description of the communications ... [this is materially identical to the third bullet point in 4.1] .

• Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate [compare the wording of the fourth bullet in 4 .2].

• The certificate that will regulate examination of intercepted material.

• An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes [identical to the fifth bullet point in 4 .2].

• A consideration of why the conduct should be authorised by the warrant is proportionate . . . [identical to the sixth bullet point in 4 .2].

• A consideration of any unusual degree of collateral intrusion . . . [identical to the seventh bullet point in 4 .2].

• Where an application is urgent . . . [identical to the eighth bullet point in 4 .2].

• An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2) -16(6) of the Act.

• An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of the Act [these last two bullets of course are the equivalent to the last bullet point in 4 .2].

... By subparagraph 4(8), the s. 8(l) warrant instrument should include 'the name or description of the interception subject or of the set of premises in relation to which the interception is to take place' and by subparagraph 4(9) there is reference to the schedules required by s. 8(2) of [the 2000 Act]. The equivalent provision in relation to the format of the s. 8(4) warrant in subparagraph 5(9) does not of course identify a particular interception subject or premises, but requires inclusion in the warrant of a 'description of the communications to be intercepted'."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

41. The applicants complained about the interception of their communications, contrary to Article 8 of the Convention:

"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."

A. The parties' submissions

1. The applicants

42. The applicants complained that, between 1990 and 1997, telephone, facsimile, e-mail and data communications between them were intercepted by the Capenhurst facility, including legally privileged and confidential material.

43. Through the statements of Mr Duncan Campbell, a telecommunications expert, they alleged that the process applying to external warrants under section 3(2) of the 1985 Act embodied five stages.

First, a warrant would be issued, specifying an external communications link or links to be physically intercepted. Such warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe". All communications falling within the specified category would be physically intercepted.

Secondly, the Secretary of State would issue a certificate, describing the categories of information which could be extracted from the total volume of communications intercepted under a particular warrant. Certificates were formulated in general terms, and related only to intelligence tasks and priorities; they did not identify specific targets or addresses. They did not need to be more specific than the broad classes of information specified in the 1985 Act, for example, "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom". The combination of a certificate and a warrant formed a "certified warrant".

The third stage in the process was filtering. An automated sorting system or search engine, operating under human control, selected communications containing specific search terms or combinations thereof. The search terms would relate to one or more of the certificates issued for the relevant intercepted communications link. Search terms could also be described as "keyword lists", "technical databases" or "The Dictionary". Search terms and filtering criteria were not specified in certificates, but were selected and administered by State officials without reference to judicial officials or ministers.

Fourth, a system of rules was in place to promote the "minimisation" of the interference with privacy, namely how to review communications intelligence reports and remove names or material identifying citizens or entities whose details might incidentally have been included in raw material which had otherwise been lawfully intercepted and processed. Where the inclusion of such details in the final report was not proportionate or necessary for the lawful purpose of the warranted interception, it would be removed.

The fifth and final stage in the process was "dissemination". Information obtained by an interference with the privacy of communications could be disseminated only where the recipients' purpose(s) in receiving the information was proportionate and necessary in the circumstances. Controls on the dissemination formed a necessary part of Article 8 safeguards.

44. The applicants contended that since the section 3(2) procedure permitted the interception of all communications falling within the large category set out in each warrant, the only protection afforded to those whose communications were intercepted was that the Secretary of State, under section 6(1) of the Act, had to "make such arrangements as he considers necessary for the purpose of securing that ... so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person" unless the requirements of section 6(2) were met. However, the precise nature of these "arrangements" were not, at the relevant time, made known to the public, nor was there any procedure available to permit an individual to satisfy him or herself

that the "arrangements" had been followed. The Tribunal did not have jurisdiction to examine such compliance, and although the Commissioner was authorised under section 8 to review the adequacy of the "arrangements" in general, he had no power to review whether they had been met in an individual case.

45. It was plain that the alleged interception of communications constituted an interference with the applicants' rights under Article 8 § 1. Any such interception, to comply with Article 8 § 2, had to be "in accordance with the law", and thus have a basis in domestic law that was adequately accessible and formulated with sufficient precision as to be foreseeable. They contended that the United Kingdom legislation breached the requirements of foreseeability. They submitted that it would not compromise national security to describe the arrangements in place for filtering and disseminating intercepted material, and that detailed information about similar systems had been published by a number of other democratic countries, such as the United States of America, Australia, New Zealand, Canada and Germany. The deficiencies in the English system were highlighted by the Court's decision in *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, which noted that the German legislation set out on its face detailed provisions regulating, *inter alia*, the way in which individual communications were to be selected from the pool of material derived from "strategic interception"; disclosure of selected material amongst the various agencies of the German State and the use that each could properly make of the material; and the retention or destruction of the material. The authorities' discretion was further regulated and constrained by the public rulings of the Federal Constitutional Court on the compatibility of the provisions with the Constitution. In contrast, in the United Kingdom at the relevant time no provision was made on the face of the statute for any part of the processes following the initial interception, other than the duty on the Secretary of State to make unspecified "arrangements". The arrangements themselves were unpublished. There was no legal material in the public domain indicating how the authorities' powers to select, disclose, use or retain particular communications were regulated. The authorities' conduct was not "in accordance with the law" because it was unsupported by any predictable legal basis satisfying the accessibility principle.

46. In addition, the applicants denied that the interferences pursued a legitimate aim or were proportionate to any such aim, since the 1985 Act permitted interception of large classes of communications for any purpose, and it was only subsequently that this material was sifted to determine whether it fell within the scope of a section 3(2) warrant.

2. The Government

47. For security reasons, the Government adopted a general policy of neither confirming nor denying allegations made in respect of surveillance activities. For the purposes of this application, however, they were content for the Court to proceed on the hypothetical basis that the applicants could rightly claim that communications sent to or from their offices were intercepted at the Capenhurst ETF during the relevant period. Indeed, they submitted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication physically intercepted under a section 3(2) warrant. However, the Government emphatically denied that any interception was being conducted without the necessary warrants and it was their position that, if interception of the applicants'

communications did occur, it would have been lawfully sanctioned by an appropriate warrant under section 3(2) of the 1985 Act.

48. The Government annexed to their first set of Observations, dated 28 November 2002, a statement by Mr Stephen Boys Smith, a senior Home Office official, in which it was claimed:

> "... Disclosure of the arrangements would reveal important information about the methods of interception used. It is for this reason that the Government is unable to disclose the full detail of the section 6 arrangements for section 3(2) warrants that were in place during the relevant period. The methods to which the relevant documents relate for the relevant period remain a central part of the methods which continue to be used. Therefore, disclosure of the arrangements, the Government assesses and I believe, would be contrary to the interests of national security. It would enable individuals to adapt their conduct so as to minimise the effectiveness of any interception methods which it might be thought necessary to apply to them.
>
> Further, the manuals and instructions setting out the section 6 safeguards and arrangements are in large part not in a form which would be illuminating or readily comprehensible to anyone who had not also undergone the training I have referred to above or had the benefit of detailed explanations. They are couched in technical language and refer to specific techniques and processes which cannot be understood simply from the face of the documents. They contain detailed instructions, precisely in order to ensure that the section 6 arrangements and section 3(2) requirements were fully understood by staff and were fully effective. Any explanations given by the Government of those techniques and processes would compound the problem, referred to above, of undermining the operational effectiveness of the system and techniques used under the authority of warrants."

The Government stressed, however, that the detailed arrangements were the subject of independent review by the successive Commissioners, who reported that they operated as robust safeguards for individuals' rights (see paragraphs 31-33 above).

49. The Government annexed to their Further Observations, dated 23 May 2003, a second statement by Mr Boys Smith, in response to Mr Campbell's statement (see paragraph 48 above), which provided more detail, to the extent that was possible without undermining national security, about the "arrangements" made by the Secretary of State under section 6 of the Act. The Government submitted that the Court should proceed on the basis that, in the absence of evidence to the contrary, in the democratic society of the United Kingdom, the relevant ministers, officials and Commissioners properly discharged their statutory duties to ensure that safeguards were in place to comply with all the requirements of section 6. Moreover Mr Boys Smith's statement showed that during the relevant period there was a range of safeguards in place to ensure that the process of selection of material for examination (the stage referred to by the applicants as "filtering") could be carried out only strictly in accordance with the statutory framework and the terms of the warrant and the certificate (that is, could be carried out only when necessary in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom), and could not be abused or operated arbitrarily.

50. According to Mr Boys Smith, all persons involved in the selection process would have had their attention specifically drawn to the safeguards and limits set out in the primary legislation, which were rigorously applied. Secondly, training was provided to all these persons to emphasise the importance of strict adherence to the operating procedures and safeguards in place. Thirdly, throughout the relevant period operating procedures were in place to ensure that it was not possible for any single individual to select and examine material on an arbitrary and uncontrolled basis. Where, as part of his

intelligence gathering, an official wished to intercept and select relevant information, he could not effect the interception himself. He would have to take the request for interception and selection to personnel in a different branch of the department, who would then separately activate the technical processes necessary for the interception and selection to be made. The requesting official would have to set out, in his request, his justification for the selection. Moreover, a record of the request was kept, so that it was possible for others (senior management and the Commissioner) to check back on the official's request, to ensure that it was properly justified. Conversely, it was not possible for the personnel in the branch of the department implementing the technical interception processes to receive the downloaded product of any interception and selection process implemented by them. Therefore, they also could not conduct unauthorised interception and gain access to material themselves. Fourth, there was day-to-day practical supervision of those who conducted the selection processes under section 3(2) warrants ("the requesting officials") by managers working physically in the same room, who could and would where necessary ask the requesting officials at any time to explain and justify what they were doing. The managers also performed quality control functions in relation to the intelligence reports generated by the requesting officials, and routinely reviewed all intelligence reports incorporating intercepted material that were drawn up by requesting officials for dissemination. Fifth, throughout the relevant period, as was explained to all personnel involved in the selection process, the independent Commissioner had an unrestricted right to review the operation of the selection process and to examine material obtained pursuant to it. From the relevant records, it was possible to check on the interception initiated by officials and, if necessary, to call for an explanation. Each of the Commissioners during the relevant period (Lords Lloyd, Bingham and Nolan) exercised his right to review the operation of the selection processes, and each Commissioner declared himself satisfied that the selection processes were being conducted in a manner that was fully consistent with the provisions of the 1985 Act. By this combination of measures there were effective safeguards in place against any risk of individual, combined or institutional misbehaviour or action contrary to the terms of the legislation or warrant. Finally, once the Intelligence Services Act 1994 had come into force on 15 December 1994, it was possible for an aggrieved individual to complain to the Tribunal.

51. As regards the processes described by the applicants as "minimisation" and "dissemination", safeguards in place during the relevant period ensured that access to and retention of the raw intercept material and any intelligence reports based on such material were kept to the absolute minimum practicable, having regard to the public interest served by the interception system. Relevant information in the material selected and examined was disseminated in the form of intelligence reports, usually compiled by the requesting officials. As part of the safeguards under section 6 of the 1985 Act, there were throughout the relevant period internal regulations governing the manner in which intelligence reports were produced, directed at all individuals engaged in producing intelligence reports based on material selected from communications intercepted under the section 3(2) warrant regime. The regulations stipulated, among other things, that no information should be reported unless it clearly contributed to a stated intelligence requirement conforming to one of the purposes set out in section 2(2) of the 1985 Act. The regulations also dealt specifically with the circumstances in which it was appropriate to name specific individuals or organisations in the intelligence reports. During the

relevant period there was in place a comprehensive security regime for handling all types of classified material. Dissemination was restricted to those with a genuine "need to know", and was further limited to persons who had been security vetted and briefed on how to handle it, with a view to ensuring continued confidentiality.

52. The Government refuted the suggestion that, to comply with Article 8 § 2, the safeguards put in place in respect of the intercepted material had themselves to comply with the "in accordance with the law" criteria. In any event, the functions of the Commissioner and the Tribunal were embodied in statutory provisions that were sufficiently certain and accessible, and in assessing whether the "foreseeability" requirements of Article 8 § 2 had been met, it was legitimate to take into account the existence of general safeguards against abuse such as these (the Government relied on *Association for European Integration and Human Rights and Ekimzhiev v. Bulgaria,* no. 62540/00, §§ 77-94, 28 June 2007 and *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994). Moreover, the 1985 Act provided that interception was criminal except where the Secretary of State had issued a warrant and sections 2 and 3(2) set out in very clear terms that, during the relevant period, any person in the United Kingdom who sent or received any form of telecommunication outside Britain could in principle have had it intercepted pursuant to such a warrant. The provisions of primary legislation were, therefore, sufficient to provide reasonable notice to individuals to the degree required in this particular context, and provided adequate protection against arbitrary interference. Article 8 § 2 did not require that the nature of the "arrangements" made by the Secretary of State under section 6 of the 1985 Act be set out in legislation (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 68), and for security reasons it had not been possible to reveal such information to the public, but the arrangements had been subject to review by the Commissioners, each of whom had found them to be satisfactory (see paragraph 33 above).

53. The Government submitted that the section 3(2) warrant regime was proportionate and "necessary in a democratic society". Democratic States faced a growing threat from terrorism, and as communications networks became more wide-ranging and sophisticated, terrorist organisations had acquired ever greater scope to operate and co-operate on a trans-national level. It would be a gross dereliction of the Government's duty to safeguard national security and the lives and well-being of its population if it failed to take steps to gather intelligence that might allow preventative action to be taken or if it compromised the operational effectiveness of the surveillance methods available to it. Within the United Kingdom the Government had extensive powers and resources to investigate individuals and organisations that might threaten the interests of national security or perpetrate serious crimes, and it was therefore feasible for the domestic interception regime to require individual addresses to be identified before interception could take place. Outside the jurisdiction, however, the ability of the Government to discover the identity and location of individuals and organisations which might represent a threat to national security was drastically reduced and a broader approach was needed. Maintaining operational effectiveness required not simply that the fact of interception be kept as secret as appropriate; it was also necessary to maintain a degree of secrecy as regards the methods by which such interception might be effected, to prevent the loss of important sources of information.

54. The United Kingdom was not the only signatory to the Convention to make use of a surveillance regime involving the interception of volumes of communications data and the subsequent operation of a process of selection to obtain material for further consideration by government agencies. It was difficult to compare the law and practice of other democratic States (such as the German system of strategic monitoring examined by the Court in the *Weber and Saravia* case cited above), since each country had in place a different set of safeguards. For example, the United Kingdom did not permit intercepted material to be used in court proceedings, whereas many other States did allow this, and there were few, if any, direct equivalents to the independent Commissioner system created by the 1985 Act. Moreover, it was possible that the operational reach of the United Kingdom's system had had to be more extensive, given the high level of terrorist threat directed at the United Kingdom during the period in question.

A. Admissibility

55. The Court notes that this 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. Whether there was an interference

56. Telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 77, 29 June 2006, and the cases cited therein). The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see *Weber and Saravia*, cited above, § 78).

57. The Court notes that the Government are prepared to proceed, for the purposes of the present application, on the basis that the applicants can claim to be victims of an interference with their communications sent to or from their offices in the United Kingdom and Ireland. In any event, under section 3(2) the 1985 Act, the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State (see paragraphs 23-24 above). Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material (see paragraph 27 above). The Court considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied (see *Weber and Saravia*, cited above, §§ 78-79).

2. Whether the interference was justified

58. Such an interference is justified by the terms of paragraph 2 of Article 8 only if it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" in order to achieve the aim or aims (see *Weber and Saravia*, cited above, § 80).

3. Whether the interference was "in accordance with the law"

a. General principles

59. The expression "in accordance with the law" under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see, among other authorities, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B, § 26; *Lambert v. France*, judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V, § 23; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX; *Dumitru Popescu v. Romania (No. 2)*, no. 71525/01, § 61, 26 April 2007).

60. It is not in dispute that the interference in question had a legal basis in sections 1-10 of the 1985 Act (see paragraphs 16-27 above). The applicants, however, contended that this law was not sufficiently detailed and precise to meet the "foreseeability" requirement of Article 8(2), given in particular that the nature of the "arrangements" made under section 6(1)(b) was not accessible to the public. The Government responded, relying on paragraph 68 of *Malone* (cited above), that although the scope of the executive's discretion to carry out surveillance had to be indicated in legislation, "the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law".

61. The Court observes, first, that the above passage from *Malone* was itself a reference to *Silver and Others*, also cited above, §§ 88-89. There the Court accepted that administrative Orders and Instructions, which set out the detail of the scheme for screening prisoners' letters but did not have the force of law, could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the relevant primary and secondary legislation, but only to "the admittedly limited extent to which those concerned were made sufficiently aware of their contents". It was only on this basis – that the content of the Orders and Instructions were made known to the prisoners – that the Court was able to reject the applicants' contention that the conditions and procedures governing interferences with correspondence, and in particular the directives set out in the Orders and Instructions, should be contained in the substantive law itself.

62. More recently, in its admissibility decision in *Weber and Saravia*, cited above, §§ 93-95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field as follows (and see also *Association for European Integration and Human Rights and Ekimzhiev*, cited above, §§ 75-77):

> "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* [*v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V]). 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)."

63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the *Weber and Saravia* case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals (cited above, § 18). The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. The Court's approach to the foreseeability requirement in this field has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in its above-cited decision in *Christie v. the United Kingdom*.

b. Application of the general principles to the present case

64. The Court recalls that section 3(2) of the 1985 Act allowed the executive an extremely broad discretion in respect of the interception of communications passing between the United Kingdom and an external receiver, namely to intercept "such external communications as are described in the warrant". There was no limit to the type of external communications which could be included in a section 3(2) warrant. According to the applicants, warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe", and all communications falling within the specified category would be physically intercepted (see paragraph 43 above). In their observations to the Court, the Government accepted that, in principle, any person who

sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication intercepted under a section 3(2) warrant (see paragraph 47 above). The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered.

65. Moreover, the 1985 Act also conferred a wide discretion on the State authorities as regards which communications, out of the total volume of those physically captured, were listened to or read. At the time of issuing a section 3(2) interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. Again, according to the applicants, certificates were formulated in general terms and related only to intelligence tasks and priorities, such as, for example, "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom" (see paragraph 43 above). On the face of the 1985 Act, only external communications emanating from a particular address in the United Kingdom could not be included in a certificate for examination unless the Secretary of State considered it necessary for the prevention or detection of acts of terrorism (see paragraphs 23-24 above). Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy.

66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials (see paragraph 43 above). According to the Government (see paragraphs 48-51 above), there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge.

68. The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in *Weber and Saravia* (cited above), express

provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (op. cit., § 32). Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act (see *Weber and Saravia,* cited above, § 100). The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications (op. cit., §§ 33-50). In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain (see paragraph 40 above), which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.

69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".

70. It follows that there has been a violation of Article 8 in this case.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

71. The applicants also complained under Article 13, which provides:

> "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."

They submitted that Article 13 required the provision of a domestic remedy allowing the competent national authority to deal with the substance of the Convention complaint and to grant relief. The 1985 Act, however, provided no remedy for an interference where there had been a breach of the section 6 "arrangements" in a particular case.

A. Admissibility

72. The Court notes that this 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

73. However, in the light of its above finding that the system for interception of external communications under the 1985 Act was not formulated with sufficient clarity to give the individual adequate protection against arbitrary interference, the Court does not consider that it is necessary to examine separately the complaint under Article 13.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

74. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

75. The applicant submitted that the application related to allegations of unlawful interception of communications over a period of approximately seven years (1990-1997), and claimed EUR 3,000 each, making a total of EUR 9,000 in respect of non-pecuniary damage.

76. The Government referred to a number of other cases involving covert surveillance where the Court held that the finding of a violation was sufficient just satisfaction (*Khan v. the United Kingdom,* no. 35394/97, ECHR 2000-V; *Armstrong v. the United Kingdom,* no. 48521/99, 16 July 2002; *Taylor-Sabori v. the United Kingdom,* no. 47114/99, 22 October 2002; *Hewitson v. the United Kingdom*, no. 50015/99, 29 May 2003; *Chalkley v. the United Kingdom*, no. 63831/00, 12 June 2003) and submitted that no financial compensation for non-pecuniary damage would be necessary in the present case.

77. In the circumstances of this case, the Court considers that the finding of violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicants.

B. Costs and expenses

78. The applicant also claimed GBP 7,596, excluding value added tax ("VAT") for the costs and expenses incurred before the Court.

79. The Government noted that counsel had acted throughout on a *pro bono* basis, and submitted that the GBP 180 hourly rate charged by Liberty was excessive. They proposed that GBP 120 per hour would be more reasonable, giving a total of GBP 5,064.

80. The Court awards EUR 7,500 plus any VAT that may be chargeable.

C. Default interest

81. The Court considers it appropriate that the default interest should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds* that there is no need to examine the complaint under Article 13 of the Convention;

4. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 7,500 (seven thousand five hundred euros) in respect of costs and expenses, to be converted into pounds sterling at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicants;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 1 July 2008, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early Lech Garlicki
Registrar President

LIBERTY AND OTHERS v. THE UNITED KINGDOM JUDGMENT