THE INFORMATION TRIBUNAL

(NATIONAL SECURITY APPEALS)

NORMAN BAKER MP (APPELLANT)

V

SECRETARY OF STATE FOR THE HOME DEPARTMENT (RESPONDENT)

DECISION

INDEX

Paragraph

INTRODUCTION

1. We were appointed members of the Data Protection Tribunal (now renamed the Information Tribunal) under section 6(4) of the Data Protection Act 1998 ("the Act") and designated by the Lord Chancellor to hear national security appeals, pursuant to Schedule 6 para. 2(1). This appeal was brought by Norman Baker MP ("the Appellant") under section 28(4) of the Act.

THE STATUTORY SCHEME

2. The significant provision of the Act is found in section 7(1) -

> 7(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled -
>
> (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
>
> (b) if that is the case, to be given by the data controller a description of -
> (i) the personal data of which that individual is the data subject,
> (ii) the purposes for which they are being or are to be processed, and
> (iii) the recipients or classes of recipients to whom they are or may be disclosed,
> (c) to have communicated to him in an intelligible form -
> (i) the information constituting any personal data of which that that individual is the data subject, and
> (ii) any information available to the data controller as to the source of those data, …".

3. In summary, an individual is entitled to be told by any person who processes personal data whether that person holds data on him (section 7(1)(a)), and if so, what the data is (section 7(1)(b)(i) and (c)(i)), why it is being processed (section 7(1)(b)(ii)) and, if known, what the source of the data was (section 7(c)(ii)).

4. Each of the material words and phrases is defined in Part I sections 1-4 of the Act. In the present context it is sufficient to say that the Security Service is a "data controller"; it processes "personal data" on individuals; and a person whose data it holds is a "data subject" for the purposes of the Act.

5. The Act requires an individual making such a request to do so in writing and, where appropriate, to pay a fee (section 7(2)). It provides for the appointment of a Data Protection Commissioner (section 6(1)), previously the Data Protection Registrar and now known as the Information Commissioner (Freedom of Information Act 2000 section 18(1)). It requires all data controllers to provide "registrable particulars" to the Commissioner (section 16(1)) who maintains a Register (section 19(1)), and it gives the Commissioner powers to enforce the Act (Part V sections 40 and following).

6. Part IV (sections 27-39) contains "Exemptions" from various provisions of the Act. The relevant exemption is "National Security" (the side-note to section 28). Section 28 provides –

> " 28(1) Personal data are exempt from any of the provisions of -
>
> (a) the data protection principles,
>
> (b) Parts II, III and V, and
>
> (c) section 55,
>
> if the exemption from that provision is required for the purpose of safeguarding national security.
>
> (2) Subject to subsection (4), a certificate signed by a Minister of the Crown certifying that exemptions from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.
>
> (3) A certificate under subsection (2) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.
>
> (4) Any person directly affected by the issuing of a certificate under subsection (2) may appeal to the Tribunal against the certificate.
>
> (5) If on an appeal under subsection (4), the Tribunal finds that, applying the principles applied by the court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may allow the appeal and quash the certificate.
>
> (6) Where in any proceedings under or by virtue of this Act it is claimed by a data controller that a certificate under subsection (2) which identifies the personal data to which it applies by means of a general description applies to any personal data, any other party to the proceedings may appeal to the Tribunal on the

ground that the certificate does not apply to the personal data in question and, subject to any determination under subsection (7), the certificate shall be conclusively determined so to apply.

(7) On any appeal under subsection (6), the Tribunal may determine that the certificate does not so apply.

(8) – (12)…….

7. We should also note that section 7(9) provides that "a court" may order the Data Controller to comply with a request made under the provisions of section 7, if it is satisfied that he has failed to do so, in breach of those provisions. Section 29 exempts inter alia personal data which is processed for the purpose of "the prevention or detection of crime" from the provisions of section 7. If the section 29 exemption is relied upon, that is in effect a statutory defence to an application under section 7(9), which has to be decided by the court to whom the application is made.

8. We on the other hand exercise only the statutory jurisdiction which is given to us by section 28. This appeal is brought under section 28(4). The second head of jurisdiction provided for by section 28(6), which has been called "subject matter jurisdiction", has not been invoked.

THE ISSUE

9. The Appellant contends that the Security Service (hereinafter "the Service"), admittedly a data controller under the Act, holds or has held personal data about him, and he has required them to say whether or not that is correct (section 7(1)(a)) and to disclose the data to him (section 7(b) and (c)).

10. The respondent to the appeal is the Secretary of State for the Home Department ("the Respondent"). He signed a Certificate dated 22 July 2000 which purports to exempt the Service from complying with the provisions of inter alia Part II of the Act, which includes section 7. The Service responded to the Appellant`s request in ambiguous terms which neither confirmed nor denied that any data were held. It also relied upon the Certificate as conclusive evidence that any data which it holds are exempt from the requirements of section 7 of the Act.

11. The Appellant appeals under section 28(4) as a person "directly affected" by the issue of the Certificate.

12. The issue therefore arises under section 28(5) - "If ..... the Tribunal finds that, applying the principles applied by the court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may allow the appeal and quash the certificate".

THE FACTS

13. On 12 July 2000 the Appellant wrote to the Director General of the Security Service (MI5) as follows –

> " Re: The Data Protection Acts 1984 & 1998 and the European Data Protection Directive.
>
> I refer to the above legal provisions. I wish to make a data subject application to yourselves under the Data Protection Acts 1984 and 1998 to inspect all data that you may hold on myself.
>
> As you will know, the Office of the Data Protection Registrar is of the view that the UK's security and intelligence agencies are duty bound to comply with the Data Protection Principles and thus the Data Protection Acts.
>
> Accordingly I would appreciate it if you would kindly now advise me as to the procedure you plan to adopt in order to process this request, and also the prospective timescale that will apply to this application.
>
> I would be grateful for acknowledgement of receipt of this letter. I look forward to hearing from you."

14. A reply from the Security Service was received on 11 August 2000:

> "Further to the Director General's of 24 July 2000, I am now writing to respond to the detail of your letter of 12 July asking for copies of records held about you by the Security Service.
>
> Under the Data Protection Act 1998 the Security Service intends to notify the Data Protection Commissioner that it processes data for three purposes. These are: staff administration, building security CCTV and commercial agreements. The Security

Service has checked its records and holds no data about you in any of these categories.

Any other personal data held by the Security Service is exempt from the notification and subject access provisions of the Data Protection Act 1998 on the ground that such exemption is required for the purpose of safeguarding national security, as provided for in Section 28(1) of the Act. Thus, if it were to be the case that the Service held any data regarding you other than for the purposes set out in paragraph 2 above, the Data Protection Act would not confer a right of access. There is therefore no data to which you are entitled to have access under the Act, but you should not assume from this letter that any such data is held about you.

I would point out that a right of appeal exists under section 28 of the Act. The section provides that the exemption described above can be confirmed by a certificate signed by a Minister of the Crown who is a member of the Cabinet, or by the Attorney General. A certificate relating to the work of the Security Service was signed by the Home Secretary on 22 July. Any person directly affected by the issuing of the certificate may appeal against the certificate to the Data Protection Tribunal…"

15. The Security Service sent the Appellant the Certificate signed by the Secretary of State for the Home Department and dated 22 July 2000.

16. Meanwhile, on 24 July 2000 the Appellant received at the House of Commons a pseudonymous letter signed by "The `Mechanic". The Appellant summarises the letter in paragraph 4 of his Witness Statement:

"This letter purported to come from someone who worked for MI5. In the letter, it was alleged that data about me was forwarded to the Security Service by East Sussex Special Branch officers in about 1998, from a source within the South Downs Earth First! Ecology group. Further the letter alleges that knowledge by Special Branch that I was involved with environmental concerns may well have lead to my details being included on the database maintained by the Animal Rights National Index (ARNI) at Scotland Yard. I am aware that allegations of misuse of interception by conducting surveillance on members of pressure groups such as Friends of the Earth and the Campaign for Nuclear Disarmament received some credence from the revelations of the former Security Service officer Cathy Massiter. Apparently my file was "closed" in mid 1989 when I commenced employment in the Liberal Democrats whips' office. However, although the file was closed, it still exists."

17. The Appellant continues (paragraph 5):

"I can confirm that I was involved in campaigning for ecological issues in East Sussex in the late 1980's. I was not involved in any criminal activities and I was not then, am not now and never have been a supporter of the use of violence and I am committed only to peaceful methods to achieve political change within a democratic society. I know nothing about the collection of data on me by East Sussex Special Branch or

anything about any proposed terrorist attacks or anything else which might come within the functions of the Security Service".

18. The principal witness for the Respondent is Mr. A.J. Tester, a senior civil servant at the Home Office. His Witness Statement begins with a summary of his evidence -

" (2) The section 28 certificate was signed by the Secretary of State pursuant to a request made to him, and on the basis of his knowledge of:-

(a) the Security Service, its functions and its primary role to protect national security, and his knowledge of the need to safeguard national security through secrecy;
(b) the safeguards and remedies open to anyone wishing to complain about any action taken by the Security Service and the alternative remedies thereby provided for those who are aggrieved by anything which he or she believes the Service has done in relation to them or their property
(c) the Data Protection Act 1998, and the intention behind section 28;
(d) past practice including the policy of successive governments to neither confirm nor deny facts relating to the operations of the intelligence and security agencies including whether they hold records on any particular individual".

19. The Information Commissioner, at a Preliminary Hearing on 30 April 2001, applied for leave to be represented at the hearing of the appeal. Her application was not opposed, and having heard submissions from counsel on her behalf we gave the following Direction:

" (4) An application by counsel for the Information Commissioner that she should have leave to be represented at the hearing was GRANTED in the following terms, in the exercise of the Tribunal's power under Rule 15(3) [of The Data Protection Tribunal (National Security Appeals) Rules 2000 S.I. 2000 No. 206 ("the Rules")]to give such directions as it thinks proper "to assist the Tribunal to determine the issues"

"The Information Commissioner shall be permitted to make a statement to the Tribunal containing such representations as she considers relevant to the Appeal, and to be represented by counsel at the hearing of the Appeal…"

subject to certain procedural conditions which were set out.

20. As stated, the Direction was made under a general power given by Rule 15(3). Its effect was not to make the Information Commissioner a party to the appeal, she not being within the statutory definition of "party" (Rule 2(3)) which is limited to the appellant, the relevant Minister and the respondent data controller. Later at the hearing we took the view

that only the parties could determine what issues were raised by the appeal, so that the Information Commissioner could not extend them. For this reason we could not entertain submissions as to whether the Security Service is required to notify with the Information Commissioner as a data controller, under Part III of the Act.

21. We should record that we were influenced in our decision to give leave to the Information Commissioner under Rule 15(3) on this occasion by the fact that this was the first appeal heard by the Tribunal under section 28 of the Act. Our decision should not be regarded as a precedent for any future appeals where a similar application is made. Such applications will be decided on their individual merits.

22. We also record we are grateful for the detailed and comprehensive Witness Statement which the Information Commissioner provided, and for the assistance we were given by Mr Henry Carr QC who represented her at the hearing. In particular she stated her position as follows:

> "My concern in the present cases is, therefore, that so far as possible the Security Service should follow good information handling practice and accordingly that the origins of data protection in fundamental rights instruments should be recognised and that arguments for disapplying the rules found in the 1998 Act should be strictly tested for proportionality"

Additionally, she described the range of response given by police forces, both in the United Kingdom and by the European Police office established by the Europol Convention (Europol) to requests for disclosure of operational data where the data may be withheld under relevant statutory provisions either wholly or in part, including cases where the existence or non-existence of data may itself not be disclosed.

THE CERTIFICATE

23. The relevant parts of the Certificate are these -

> " I, the Right Honourable Jack Straw MP, one of her Majesty's Principal Secretaries of State, in exercise of the powers conferred by the said section 28(2) do issue this certificate and certify as follows:-

1. that any personal data that is processed by the Security Service as described in Column 1 of Part A in the table below are and shall continue to be required to be exempt from those provisions of the Act that are set out in Column 2 of Part A;

2. [a corresponding provision referring to Part B: no separate issue arises in relation to this];

3.....

4.....

all for the purpose of safeguarding national security.

PART A

Column 1

1. Data processing in performance of the functions described in Section 1 of the Security Service Act as amended by the Security Service Act 1996 including but not limited to:

(i) obtaining personal data from human sources being agents or contacts of the security service;

(ii) obtaining personal data from other United Kingdom government departments, agencies or public authorities;

(iii) obtaining personal data from security and intelligence agencies, law enforcement agencies and other liaison contacts of other governments;

(vi) recording, holding, organising, adapting, altering, retrieving, consulting, aligning, combining, blocking, erasing, destroying and otherwise using such data;

(vii) transmitting such data to and from and between Security Service Stations overseas;

(viii) disclosing or disseminating such data to other United Kingdom government departments, agencies or public authorities.

Column 2

(i) Part II;

(ii) Part III;

(iii) Part V;

(iv) Section 55;

(v) The first data protection principle;

(vi) The second data protection principle;

(vii) The sixth data protection principle to the extent necessary to be consistent with the exemption contained in this certificate;

(viii) The eighth data protection principle

24. The width of the exemptions required by Column 2 is illustrated by quoting the headings of the Parts of the Act that are referred to -

Part II - Rights of Data Subjects and Others

Part III - Notification by Data Controllers

Part V - Enforcement

(Note: this Part includes section 42, which entitles any person who is, or believes himself to be, directly affected by any processing of personal data to

request the Information Commissioner`s assistance)
section 55 - (side note) Unlawful obtaining etc. of personal data.

25. The terms of the Certificate are detailed and carefully drafted. The scope of the exemptions claimed varies from one category of personal data to another, and it is clear that full consideration was given to what was in the view of the Respondent the minimum scope required for each. Nevertheless, the effect of paragraph 1 of the Certificate coupled with Columns 1 and 2 of Part A can fairly be described as a blanket exemption for "any personal data that is processed by the Security Service" in the performance of its statutory functions. We draw attention to the fact that whereas the certificate is issued "for the purposes of safeguarding national security" it does not on its face limit the Service's use of it to particular cases where national security is engaged.

26. The present certificate is both general and prospective. We have to bear in mind, however, that neither generality nor prospectivity can in themselves be grounds of attack.

27. A question arises as to the scope and true construction of this Certificate, although it was not pressed in argument before us. Paragraph 1 of the Certificate exempts "any personal data that is processed by the Security Service" from the requirements of inter alia Part II of the Act. These requirements include, as we have noted above, the individual`s right under section 7(1)(a) "to be informed.....whether personal data of which the individual is the data subject are being processed by or on behalf of that data controller". "Personal data" is defined in section 1(1), the relevant words being "data which relate to a living individual".

28. It can be argued therefore that since a request under Section 7(1)(a) raises the very question whether personal data are being processed, and since the Certificate on its face exempts only personal data that is processed by the Security Service from the subject access obligations under Section 7, the Certificate does not exempt the Service from the duty under Section 7(1)(a) to inform the individual whether or not relevant data are being processed (which includes held) unless the data do in fact exist.

29. Notwithstanding this difficulty in the literal construction of the Certificate, read in conjunction with the Act, we are satisfied that the exemption purported to be given does

include the duty to respond to a request under section 7(1)(a), whether or not data in fact exists. We are clear that the Certificate was intended to, and on its true construction does, exempt personal data "if any" that is processed by the Service, especially since the exemption purported to be given by Part A Column 2 includes the provisions of Part II of the Act, and these include section 7(1)(a), apparently in all cases where the request is made.

THE NCND POLICY

30. By exempting the Security Service from the duty under section 7(1)(a) of the Act to inform the individual making the request whether or not his personal data are being processed, the Certificate authorises the non-committal reply which was given to Mr. Baker. This means that both the Certificate and the response gave effect to the policy which is known colloquially as `neither confirm nor deny` and by the acronym `NCND'. We have no doubt that they were intended to do so.

31. The Respondent acknowledges the existence of this policy, and his primary contention is that it is justified by the need to safeguard national security. Indeed, much of the evidence placed before us was directed towards the question whether such a policy is consistent with the obligations of a modern democratic State to respect the private rights of individuals who make requests of the kind contemplated by section 7 of the Act. In the event, however, as we will relate below, that is not the issue we have to decide. Rather, the appeal is concerned with the application of the policy, and specifically with the question whether the Respondent had reasonable grounds for authorising the Service to respond with a NCND reply to every request made to it under section 7(1)(a), unless the Service decides to make an exception in a particular case. For that is the effect of the Certificate, as we have held it to be, and if the NCND response is permitted in all cases then the practical result is that the Service is not obliged to consider each request on its individual merits. That follows if the NCND reply is invariably justified, and we were furnished with no evidence that individual consideration is given to the possible consequences of making a positive response to every request.

32. The Respondent contends that he had reasonable grounds for issuing a Certificate

which gives the Service a blanket exemption from the provisions of section 7 of the Act and which permits the NCND reply generally. The Appellant supported by the Information Commissioner submits that the Certificate should not relieve the Service from the duty to give separate consideration to each request, whilst recognising that in many cases the NCND reply may be justified in the circumstances of that case. So much so indeed, that the Service may respond with a NCND reply to every request made to it.

ADMITTED EXCEPTIONS

33. There are some well-established circumstances in which the Service does acknowledge that information has been collected and is still held. Sometimes, the information may be released. These circumstances, as Mr. Burnett QC put it in his oral submissions to us, can be grouped together as cases where the person concerned already knows "conclusively" that there is information held upon him. Another situation which can arise is where the Service itself decides that the acknowledgement should be made, and even that the information should be published, because that is seen as assisting the proper performance of its statutory functions, or as otherwise being in the public interest. This too becomes a case of "official confirmation" that the information is held. These and similar cases, Mr. Burnett Q.C. submits, are "well recognised exceptions" to the policy of answering requests with some variant of the formula NCND. They are "dictated by common sense".

34. This group of cases (which is not closed) includes -

"(a) Members or former members of agencies who know that data are held.

(b) Individuals who are subject to removal from the United Kingdom on Grounds of national security who have become conclusively aware of Security Service interest in them.

(c) Those involved in criminal proceedings who have conclusively become aware of Security Service interest in them.

(d) Others in whom Security Service interest has been publicly confirmed in [Court or other] proceedings."

We shall call these the " admitted exceptions" to the NCND policy.

GENERAL OBSERVATIONS

35. (1) It is common ground between the parties, and the Information Commissioner agrees, that in general the work of the Service must be carried out in secret, and that to a large extent its records must be kept secret also, including the fact that individual files exist.

(2) This secrecy is necessary in order to safeguard national security, whose importance as a policy objective in the contemporary world cannot be overestimated.

(3) The Appellant recognises that the NCND response to a subject access request is justified in certain cases. These are -

(a) when no data are held in fact and therefore no file exists. The NCND policy is justified in this case because if one person was correctly given a negative answer to his request, another person who received a NCND reply might deduce, correctly or otherwise that personal data was held about him. The second person might be an associate of the first e.g. in a terrorist organisation;

(b) when data are held, and the Service lawfully decides that a positive response or disclosure of any of the data would endanger national security in that particular case. This presupposes that individual consideration is given to the request;

(c) when data are held, and the Service is willing to acknowledge the existence of some of that data, and maybe also to release part of the data, to the person making the request, but it also decides, lawfully, that the existence of the remaining data should not be disclosed. In such cases, a modified form of NCND reply might state "Beyond what is disclosed, the Security Service does not process any data which you are entitled to receive" or some other variant of the Europol reply. (Mr Carr QC, for the Information Commissioner, suggested "The information which the Security Service is required to supply under the provisions of the Act is enclosed.)

(4) The remaining case is where data are processed (held) but the Service is unwilling to acknowledge its existence. This could arise if a justifiable decision was made that national security would or might be harmed by a positive response. But if the NCND reply is permitted in all cases, these could include ones where the Service made no decision on the particular request (if it could rely on a blanket exemption, it would not be obliged to do so), and others where a decision was made but was unjustified. The person making the request would then have no means of knowing whether a decision was taken, and if it was, whether it was justifiable or not.

(5) In short, we repeat, by certifying that the Service is exempt from the requirements of section 7(1)(a) of the Act, the Respondent has released it from any obligation to consider each request on its individual merits. The blanket exemption purportedly permits the Service to give a NCND reply to every request, and if the Certificate was issued on reasonable grounds the person directly affected by it has no means of challenging such response under the Act. At its most extreme, the Respondent's submission indeed means that the Tribunal effectively has no power to consider individual cases under section 28(4).

(6) The Certificate dated 22 July 2000 was said in the Respondent`s evidence to have been signed "pursuant to a request made to him" (Tester para. 2). This does not mean that it was signed in response to the Appellant`s request, although the dates might suggest that it was (see above). Mr. Burnett QC for the Respondent told us the dates are a coincidence, and he confirmed that the Certificate was intended to be used as a general response and for future cases also. As we have noted, this is permitted in terms by section 28(3) of the Act.

(7) Mr. Nicol QC therefore submitted that the primary issue in the appeal is whether the Respondent had reasonable grounds for issuing a Certificate which authorises the Service to respond with a NCND reply in every case, without necessarily deciding whether a positive response would endanger national security in the individual case.

(8) Mr Carr QC supported this submission, "focusing on the question, is it [reasonably] necessary or required for the purposes of national security, to have a blanket certificate, which as Mr Nicol has pointed out will in fact prevent [sc.permit non-] disclosure of everything, even in the innocuous case".

(9) It could be said that the certificate is not of itself unreasonable; it merely puts a weapon in the hands of the Security Service to use or not use as they see fit. They are not obliged to use it in any particular circumstance. We do not consider that this would, however, exculpate a certificate that was otherwise flawed.

JURISDICTION AND POWERS

36. When Mr. Nicol QC concentrated his attack on the "issue" of the Certificate, it became apparent that the Service`s response to a section 7 request involves two steps. First, the issue of the Certificate by the Respondent. Secondly, the Service`s own decision to rely upon it in the particular case. Notwithstanding the coincidence of dates, to which we have referred in paragraph 27 (6) above, this was true of the Appellant`s request also. We can infer that the Certificate was obtained in response to his letter dated 12 July 2000, but this was only because it was the first request that the Service received, or the first that it decided should be answered in this way. The decision to use it was its own and was entirely separate from the issue of the Certificate by the Respondent for use in this and other cases where the Service wishes to give a non-committal answer.

37. This leads to the question whether we have power to judicially review the Service`s decision to rely upon the Certificate in this case. We are clear that we do not. Section 28(5) confines us to the issue i.e. signing of the Certificate by the Minister, and we cannot extend this to include another agency`s decision to rely upon it in a particular case. When that other agency is the data controller, the data subject may have other remedies under the Act (see e.g. sections 7(9), [29] and 40 (the Information Commissioner)). He may also be able to bring proceedings for judicial review of that decision before the Administrative Court. But our jurisdiction is expressly limited to the "issuing" of the Certificate by the Minister, who is the respondent to this appeal.

38. Here we should revert to the terms of sections 28(4) and 28(5) of the Act, which defines both our jurisdiction and our powers. We have to be satisfied that the Appellant is a person "directly affected". We have to find whether or not the Minister had reasonable grounds for issuing the Certificate. We must apply the principles applied by the court on an application for judicial review. Finally, if we find that the Minister did not have reasonable grounds, we may allow the appeal and quash the Certificate.

39. Each of these requirements raises questions of interpretation.

(1) Who is a person "directly affected"?

(2) Does "reasonable grounds" include an issue as to whether the Minister went beyond his legal powers when he signed the Certificate?

(3) What are the principles of judicial review that we must apply?

(4) What is the significance of the Tribunal`s powers under section 28(5), these being expressed with the permissive “may”?

(5) Do we have power to “quash” the Certificate in part, or in relation to the present case only?

40. We will take these questions of interpretation in turn and consider them in relation to the present case. Since this is the first substantive appeal that the Tribunal has heard and we have had the benefit of submissions of high quality, we will add more general comments where we feel that it may be useful to do so.

(1). <u>"Directly affected"</u>

41. It was common ground, rightly in our judgement, that the Applicant is a person "directly affected", as someone seeking to exercise his Section 7 (1) (a) rights and blocked by the certificate in his attempt to do so. Section 28 (4) distinguishes between persons directly and persons only indirectly affected by issue of the certificate : the Appellant is manifestly in the former category.

(2) Legality

42. The Certificate purports to grant exemption from the provisions of inter alia section 7 of the Act to "Data processing [by the Service] in performance of the functions described in section 1 of the Security Service Act 1989 as amended by the Security Service Act 1996....." (Part A Column 1 para. 1). The exemption is given "for the purpose of safeguarding national security"

43. Section 1 of the Security Service Act 1989 in its original form read as follows –

> " (1) There shall continue to be a security service (in this Act referred to as "the Service" under the authority of the Secretary of State.
>
> (2) The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
>
> (3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

44. The 1996 amendments added the following sub-section –

> "(4) It shall also be the function of the Service to act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime."

45. We need not dwell overlong on the interpretation of this section, as amended. It is uncontrovertible that on its true construction the functions of the Service now extend beyond matters which affect national security. They "also" include "safeguarding the economic well-being of the United Kingdom" against external threats, and work in the prevention and detection of serious crime, whether or not any threat to national security is involved. Parliament clearly saw these functions as additional to the protection of national security (whatever the precise meaning of that phrase) and intended that the Service should have

them. All these functions may overlap, but equally they may not do so. They interrelate, but they do not coincide. There may therefore be cases of data processing by the Service where national security, however defined, is not at risk, but which since 1989 have come within the scope of the Service`s statutory functions.

46. The contention that the Certificate is unlawful because widely expressed is developed as follows. The statutory functions of the Service "as described" in the Security Service Acts, as referred to in the Certificate, include some which may but do not necessarily involve considerations of national security i.e. sub-sections (3) (1989) and (4) (1996) of section 1 as amended, yet the Certificate purports to exempt "any personal data that is processed by the Security Service", which implies that the exemption covers all personal data that are processed in the performance of any of its functions. Therefore, it is argued, the exemption is wider than is required for the purpose of safeguarding national security, and so the Minister exceeded the power given to him by section 28 of the Act.

47. If this is correct as a matter of construction, a further question arises as to the scope of our jurisdiction under section28(5). We are required to consider whether the Minister had reasonable grounds for issuing the Certificate. Does this include consideration of whether he exceeded his lawful powers in doing so? Mr. Nicol QC submits that an unlawful act must always be held unreasonable, and therefore the legality or otherwise of the Certificate must certainly be relevant to our consideration of reasonableness. Mr. Burnett QC was not disposed to quarrel with this submission, and the issue of law was not fully argued before us. Nevertheless, we have given further thought to it, not least because it could affect our jurisdiction, if the contention outlined above is correct.

48. There are substantial arguments, it seems to us, in support of both, conflicting views. On the one hand, as Mr. Nicol submits, if a Minister acts unlawfully, he can readily be said to be acting without reasonable grounds. (However, logically at least, this may not be invariably correct). Moreover, there is the practical consideration that if the Tribunal has no power to determine whether the Certificate was issued lawfully, that issue would have to be decided in parallel proceedings elsewhere, presumably in the Administrative Court.

49. On the other hand, statements of the principles of judicial review, which we have to apply, habitually have distinguished between unlawfulness (illegality) and unreasonableness (irrationality) as grounds for interference by the Court. True, the recent authoritative statements of principle which have followed the incorporation of the European Convention of Human Rights ("the ECHR") into English law, emphasize the flexibility of the principles applied by the Courts. But the classic statement in Council of Civil Service Unions v. Minister for the Civil Service [1985]AC 374, by Lord Diplock at 409, identified three discrete grounds of challenge: illegality, procedural impropriety and irrationality (and hinted at a fourth, lack of proportionality).

50. The principles, we must assume, were well known to Parliament when section 28(5) was passed into law, in terms which limit the Tribunal`s jurisdiction to deciding whether the Minister had reasonable grounds. It might therefore be necessary to infer that Parliament intended that questions as to the legality of a Certificate should not be entrusted to the Tribunal but should remain with the Courts. But, as against this, we note that members of the Tribunal designated to hear national security appeals must be lawyers: section 6 and Schedule 6 of the Act.

51. The debate assumes that a clear distinction can be made between the lawfulness of a Certificate and the question whether there were reasonable grounds for issuing it, or at least that a distinct issue as to legality arises in the particular case. We are clear that the distinction, if one exists, does not depend upon which of its statutory functions the Service was performing when it processed the personal data in question. A Certificate exempts the Service from the provisions of inter alia section 7 of the Act. The exemption, if it is lawful, is required for the purpose of safeguarding national security. The potential harm to national security which the Certificate is intended to avoid therefore arises from the consequences of disclosure, whether of the personal data itself or of whether or not it exists, at the time when the request for its release is made. As Mr. Burnett submitted, and the Respondent`s evidence makes clear, a positive response could be harmful to national security even where the personal data, if any, which the Service is processing was acquired, or is being held, in the exercise of its functions where national security is not involved, for example , safeguarding the economic well-being of the United Kingdom or inquiring into serious crime. This may be true of the data itself, or of the sources from which it was acquired, or of the methods or

techniques that were used. The same sources may tell the Service about spies as well as drug dealers. The same surveillance techniques may be used for either category of malefactor. If the NCND policy could not be operated in cases where the Service was involved for reasons other than national security, a terrorist might infer from its use against him that his personal data might be held; or a criminal could discover whether he was known to be or was suspected of being a terrorist also.

52. For these and maybe other reasons, the question whether a Minister had reasonable grounds or not for issuing a Certificate is distinct from the question as to the nature of the Service`s activities which have resulted in personal data (if any) being processed by it. The consequences of disclosure have to be assessed independently of the purpose for which the data (if any) were acquired or are being held. The fact that data are processed for a reason unconnected with national security does not mean that the exemption cannot be justified "for the purpose of safeguarding national security" when the request is made.

53. The legality argument arises if the terms of the Certificate are wide enough to exempt the Service from the provisions of the Act even in a case where a claim that national security would be harmed if the Act was complied with cannot be justified. But that argument is secondary to the question whether the Minister had reasonable grounds for granting an exemption which de facto relieves the Service from any obligation to give separate consideration to each individual request. If we conclude that the Certificate should be quashed on that wider ground, the legality issue does not arise for decision in the present case.

54. In this context we should mention a particular feature of this case. The Appellant relies upon evidence that his activities were the subject of investigation over a short period which ended in 1989. The evidence consists of the letter he received from `the Mechanic', after he made his request, and his own account of his and his associates` activities during that period, which he contends could have attracted the interest of the Service, though he does not accept that national security was at risk. He has been told by `the Mechanic' that the inquiries affecting him were terminated in 1989 for the fortuitous reason of his political advancement in that year. He does not know whether or not that is correct, because he has received only the non-committal reply which has given rise to this appeal.

55. This evidence in our view establishes a prima facie case that the Service did process personal data on the Appellant during the years 1986-1989 and that it still does so, but since 1989 only by reason of continuing to hold data about him. We do not know in fact whether this is correct, and for reasons which appear below we have not found it necessary to seek to inquire further into it.

56. Before 1989, there was no statutory regulation of the Security Service, nor even any statutory recognition of its existence. During the period 1986 - 1989, therefore, it did not have any statutory functions. It was not argued before us that, for this reason, the Certificate (even if lawful) does not exempt in fact what was done before 1989. If the point had been raised, there were, in our view, two convincing answers to it. First, the Certificate exempts data processing "in performance of functions of the kind described in paragraph 1 of Part A, Column 1", whenever they were performed, and secondly, data acquired before 1989 have continued being processed by being 'held' since that date. In this case, therefore, the legality issue would only arise where the Service processed personal data on the Appellant before 1989, if it did so for reasons other than considerations of national security. Any processing which has taken place since 1989 ie by holding rather than obtaining data has been permitted by section 1(c) of the 1989 Act; similarly by section 1(d) since 1996. The need to investigate these matters, which we have not done nor been invited to do, underlines our conclusion (paragraph above) that the legality issue is secondary to the principal issue raised by this appeal

3) The Principles of Judicial Review.

57. It was common ground before us that section 28(5) requires the Tribunal to apply the principles of judicial review as they are applied by the courts at the time of the appeal hearing. We agree with this approach, which seems to us to be the natural meaning of the phrase in its statutory context. Moreover the Data Protection Act 1998, like other legislation, must be read 'so far as it is possible to do so' in a manner which protects convention rights (Human Rights Act 1998 s.3. see generally R v A (HL), [2001] 2 WLR 1546 at pp. 1562-3 (para. 44: p1582 (para. 108)). We cannot contemplate that section 28(5) intended that the Tribunal should apply indefinitely the principles which were already established in 1998, without regard to later developments in them. We therefore have to take account of the

impact which the Human Rights Act has had on the principles of judicial review, particularly the need to recognise and incorporate in them the notion of proportionality.

58. Before we consider the reach of those principles, we draw attention to the international law context of the Act.

59. When the Appellant applied to the Security Service he did so under the Act and under the European Community Data Protection Directive ("the Directive"), made by the European Parliament and the Council on 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive followed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted by the Member States of the Council of Europe, including the United Kingdom, on 28 January 1981 ("the 1981 Convention"). It was pursuant to the 1981 Convention that the United Kingdom enacted the Data Protection Act 1984 - see R v Brown [1996] 1 All ER 545 per Lord Hoffmann at 556. This has now been superseded by the Act. The Act is the transposition of the Directive into United Kingdom domestic law.

60. The Directive has 72 preambles. These make clear that the Directive is to give substance to and amplify both the rights contained in the 1981 Convention and the rights recognized in Article 8 (respect for private life) of the ECHR. The ECHR of course is also given further effect to in UK law by the Human Rights Act 1998 ("the HRA").

61. It is unnecessary to consider the operative provisions of the Directive in any detail. Particular reference may be made to Article 3, which defines the scope of the Directive; Article 12, which deals with rights of access; and Article 13, which contains exemptions, including in respect of national security, when this constitutes a "necessary measure" (in a democratic society).

62. In accordance with established principle the Act must be construed - so far as it is possible to do so - so as to accord with the Directive, and indeed the Directive itself is directly enforceable against the Respondent as an emanation of the State. There does not, however, appear to be an issue of pure construction in the present proceedings, and we do not need to consider in what forum a person might seek to establish rights (if any) arising only under the Directive. Moreover, and importantly, in the context of the present issue the Act,

like other legislation, must be read so far as it is possible to do so in a manner which protects ECHR rights: see Section 3 of the HRA and the decision of the House of Lords in R v A (No 2) [2001] 2 WLR 1546, especially per Lord Steyn at 1562H-1563G.

63. We have accordingly asked ourselves the question: is the issue by the Secretary of State of his certificate reasonable in the extended sense of proportionate by reference to the precepts of the ECHR: see Sections 1 (1) (a), (2) and (3) and Schedule 1, 2 and 6(2)(a) of the HRA.

64. The material ECHR provision is Article 8, referred to above. It provides:-

> "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 wellbeing 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."

65. ECHR case law to which we were helpfully referred in connection with the relationship between respect for private life and the demands of national security included Klass v Germany (1978) 2 EHRR 214; Esbester v UK (1993) 18 EHRR (CD) 72; Kopp v Switzerland (1998) 27 EHRR 91; Leander v Sweden (1987) 9 EHRR 433; Amman v Switzerland (2000) 30 EHRR 843; and Rotaru v Romania (Application 28341/95, Judgment 4.5.00).

66. The following questions are posed:

(i) Is there an interference with the right to respect for the Appellant's private life in the application to him of the 'neither confirm nor deny' (NCND) policy?

(ii) If so, is that interference in accordance with the law?

(iii) If so, does it pursue a legitimate aim?

(iv) Is it necessary in a democratic society ie proportionate?

67. At first blush it is not apparent how a refusal to confirm or deny that records are kept about the Appellant interferes with respect for his private life. The ECHR case law referred to above identifies that both the holding of information and the refusal to allow access to it, to enable any necessary refutation, qualify as interferences. NCND, however, is distinct from either of these two matters. If no files are kept, there is nothing to refute. We are, however, persuaded that to approach the matter in this way would be over technical. Knowledge as to whether files are held is a precondition of action by the data subject. Denial of that knowledge may prevent him taking action which he would otherwise take, ie by access and refutation. Moreover, the 1981 Convention by Article 8A and the Directive (see para 61 above) identify a NCND policy as something which requires justification. In any event in this particular case there is evidence consistent with the Appellant's own statement which raises a sufficient case that he may be being denied access to an existing file.

68. The submission that the interference was not in accordance with the law focussed upon the alleged lack of clarity in the expression 'national security'. We reject this submission. The Tribunal accept that in this context legality means not only compliance with domestic law, but compliance with principles of justice such as clarity and accessibility. However, despite the fact that the Strasbourg organs have had to consider Article 8 claims where reliance is placed on national security (or cognate) interests by the Defendant state, it has never been suggested, at any rate in any majority judgement, that the concept is so vacuous as to fail the test of clarity. The phrase itself is found in the 1981 Convention, in the Directive, and in the statutes and codes of Member States. The fact that it is incapable of comprehensive definition does not mean that it lacks adequate definition.

69. The pursuit of a legitimate aim, ie national security, is conceded.

70. The concept of proportionality is the key issue. It has received recent and authoritative analysis in decisions of the Privy Council, De Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69 ("De Freitas"), and the House of Lords, R (Daly) v Secretary of State for the Home Department [2001] 2 WLR 1622 ("Daly"). While in different contexts the concept may have different meanings, we consider that this

analysis is pertinent to our function, and propose to adopt it.

71. The consequences in terms of applicable judicial review principles has also been set out in Daly. Lord Steyn said, at 1635B-1636A, having referred to the three-stage test adopted in De Freitas:

> "Clearly these criteria are more precise and more sophisticated than the traditional grounds of review. What is the difference for the disposal of concrete cases? Academic public lawyers have in remarkably similar terms elucidated the difference between the traditional grounds of review and the proportionality approach: ... The starting point is that there is an overlap between the traditional grounds of review and the approach of proportionality. Most cases would be decided in the same way whichever approach is adopted. But the intensity of review is somewhat greater under the proportionality approach. Making due allowance for important structural differences between various convention rights, which I do not propose to discuss, a few generalisations are perhaps permissible. I would mention three concrete differences without suggesting that my statement is exhaustive. First, the doctrine of proportionality may require the reviewing court to assess the balance which the decision maker has struck, not merely whether it is within the range of rational or reasonable decisions. Secondly, the proportionality test may go further than the traditional grounds of review inasmuch as it may require attention to be directed to the relative weight accorded to interests and considerations. Thirdly, even the heightened scrutiny test developed in R v Ministry of Defence, Ex p Smith [1996] QB 517, 554 is not necessarily appropriate to the protection of human rights. It will be recalled that in Smith the Court of Appeal reluctantly felt compelled to reject a limitation on homosexuals in the army. The challenge based on article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the right to respect for private and family life) foundered on the threshold required even by the anxious scrutiny test. The European Court of Human Rights came to the opposite conclusion: Smith and Grady v United Kingdom (1999) 29 EHRR 493. The court concluded, at p 543, para 138:
>
> "the threshold at which the High Court and the Court of Appeal could find the Ministry of Defence policy irrational was placed so high that it effectively excluded any consideration by the domestic courts of the question of whether the interference with the applicants' rights answered a pressing social need or was proportionate to the national security and public order aims pursued, principles which lie at the heart of the court's analysis of complaints under article 8 of the Convention."

In other words, the intensity of the review, in similar cases, is guaranteed by the twin requirements that the limitation of the right was necessary in a democratic society, in the sense of meeting a pressing social need, and the question whether the interference was really proportionate to the legitimate aim being pursued."

72. In Daly, Lord Cooke of Thorndon said, at 1636G-1637C:

> "The other matter concerns degrees of judicial review. Lord Steyn illuminates the distinctions between "traditional" (that is to say in terms of English case law, Wednesbury) standards of judicial review and higher standards under the European Convention or the common law of human rights. As he indicates, often the results are the same. But the view that the standards are substantially the same appears to have reached its quietus in Smith and Grady v United Kingdom (1999) 29 EHRR 493 and Lustig-Prean and Beckett v United Kingdom (1999) 29 EHRR 548. And I think that the day will come when it will be more widely recognised that Associated Provincial Picture Houses Ltd v Wednesbury Corpn [1948] 1 KB 223 was an unfortunately retrogressive decision in English administrative law, in so far as it is suggested that there are degrees of unreasonableness and that only a very extreme degree can bring an administrative decision within the legitimate scope of judicial invalidation. The depth of judicial review and the deference due to administrative discretion vary with the subject matter. It may well be, however, that the law can never be satisfied in any administrative field merely by a finding that the decision under review is not capricious or absurd."

73. It is clear that where convention rights are engaged, judicial review principles may require a more intrusive judicial attitude than conventional Wednesbury or even heightened Wednesbury. However Lord Steyn added a significant footnote to his exegesis, at 1636A-C:

> "The differences in approach between the traditional grounds of review and the proportionality approach may therefore sometimes yield different results. It is therefore important that cases involving Convention rights must be analysed in the correct way. This does not mean that there has been a shift to merits review. On the contrary, … the respective roles of judges and administrators are fundamentally distinct and will remain so. To this extent the general tenor of the observations in Mahmood [2001] 1 WLR 840 are correct. And Laws LJ rightly emphasised in Mahmood, at p 847, para 18, "that the intensity of review in a public law case will depend on the subject matter in hand". That is so even in cases involving Convention rights. In law context is everything."

74. As to the margin of discretion for the decision maker and comparison with other systems generally and in particular in respect of national security, reference may also be made especially to the cases referred to at para 39F above, and Gardels v CIA (1982) 689 F 2d 1100 and Brown v Stott (2001) 2 WLR 817 [2001] SLT 59 (Privy Council), especially at 69/70, per Lord Bingham.

75. From this three conclusions can be drawn:

(i) Judges operating judicial review principles are not second stage administrators, even in ECHR territory. Theirs is a review, not an appellate role. So a margin of judgement is to be allowed to the administrator.

(ii) The intensity of judicial supervision is always dictated by context.

(iii) This is so 'even' where ECHR rights are invoked.

76. It seems to us from this passage that this Tribunal must remain sensitive to the issue underlying these proceedings; when does national security take precedence over human rights? Where the context is national security judges and tribunals should supervise with the lightest touch appropriate; there is no area (foreign affairs apart) where judges have traditionally deferred more to the executive view than that of national security; and for good and sufficient reason. They have no special expertise; and the material upon which they can make decisions is perforce limited. That the touch should be the lightest in comparative terms does not, of course, assist in weighing up how light that should be in absolute terms. While we note from Mr Nicol QC's compendium that the security services and security operations have been increasingly circumscribed by legal rules and procedures, eg the Special Immigration Appeals Commission Act 1997, Section 41 of and Schedule 8 to the Employment Relations Act 1999, Schedule 3 to the Terrorism Act 2000 (The Proscribed Organisations Appeal Commission), and Sections 7 and 8 of the Race Relations (Amendment) Act 2000, our exercise of quasi-judicial power ultimately is limited, as well as created, by the language of s.28(4). We must apply judicial review principles in a manner appropriate to the national security context: no less, but no more.

(4) <u>Discretion</u>

77. If the finding is made of 'no reasonable grounds', the Tribunal "may" allow the appeal and quash the Certificate. Both parties accepted before us that the sub-section gives the Tribunal a discretion which has to be judicially exercised, whether to quash the Certificate or not, but does not impose a duty to do so.

78. One obvious case for abstinence by the Tribunal might be where the certificate was spent. However, to quash a certificate does not immediately compel disclosure of information still thought to imperil national security. It is only when a successful application is made to a Court to enforce it (Data Protection Act 1998 s.7(9)), by which time an ex hypothesi valid certificate may have been issued, that disclosure is compelled. We note that unlike the Administrative Court we have no power to make a declaration as an alternative to a quashing order. Therefore, the considerations which could affect the Tribunal's decision are not necessarily the same as those which would be taken into consideration by the Court

(5) The power to quash

79. We have referred above to the question that arises as to the extent of our power to "quash" the Certificate, if we have found that the Minister did not have reasonable grounds for issuing it. The issue is whether the power to "quash" enables us to quash part but not the whole of the document. We note that Certiorari is the quashing remedy in judicial review. Wade & Forsyth Administrative Law (8th ed) at p.591, says that if a decision does not pass the test (sc of validity), it is quashed - that is to say it is declared completely invalid, so that no one need respect it.[1] The by-law cases ditto (pp. 866-7) contemplate partial invalidity. At best, these would be analogies; "quashing" is the statutory word here implying, it could be said, that it is unqualified and thus means wholly only. Alternatively it could be said that the greater necessarily includes the latter, and thus means wholly or partly. In so far as this is a matter of impression, we prefer the former construction. No particular harm would result from such a construction, since quashing a certificate does not expose the data controller to an immediate obligation to disclose the existence of, let alone the material which he considers would imperil national security. We certainly have no power to rewrite a certificate.

80. We have borne in mind that Rule 28(4) refers to quashing "whether in whole or in part". Delegated legislation must of course be in harmony with primary legislation, it cannot ordinarily, unless the primary legislation expressly so provides, dictate its meaning. Neither counsel submitted that the Rule enlarged our powers or compelled the conclusion that we could quash in part, and we are content to accept the drafting of the rule as not undermining our reasoning.

---

[1] Lewis, *Judicial Remedies in Public Law*, however contemplates partial quashing (2nd ed. at p. 153).

REASONABLE GROUNDS

81. The Respondent`s reasons for issuing the Certificate are set out in Mr. Tester`s Witness Statement, supported by Statements from five members of the Service. His evidence in summary is that careful consideration was given to the extent of the exemption that was reasonably required by the Service in relation to different categories of personal data held by it, hence paragraphs 1-4 of the Certificate and the corresponding Parts A-D. The Respondent was motivated by the need to ensure that the Service could operate in conditions of secrecy, for reasons which were fully explained in the supporting Witness Statements. He relied upon the protection given by other statutory agencies to any individual who complains of misconduct by the Service. He took account of the position in other countries. All States and international instruments recognise the requirements of national security as paramount, and States are allowed a large margin of appreciation in deciding what degree of protection is necessary and justified. Many other States operate one form or another of a NCND policy when responding to requests for personal data (including requests as to the existence of data) when national security is involved. NCND has been the policy and practice of successive governments of this country.

82. Much of the material put before us, by the parties and by the Information Commissioner, is concerned with the history of and justifications for the NCND policy, both in this country and in other States. We do not find it necessary to consider this evidence in detail. The Appellant accepts that the policy is both necessary and justified in very many, perhaps even the great majority of cases where the Service is requested to disclose information or whether personal data is being accumulated or held. Secrecy is essential to their operations, and it may be vital that the veil of secrecy should protect the Service`s agents and informers and the methods and techniques they use or have used.

83. None of this is in dispute, nor is the fact that the Service itself is best-placed to decide whether or not, and if so, to what extent, the NCND policy should be applied in an individual case. The issue raised by this appeal is whether it is reasonable and proportionate for the Service to apply the policy in every case; whether it should be authorised to answer every request in this way, even if in a particular case the request could be given a positive rather than a non-committal answer without harming national security.

84. Such cases do exist. One category is described in Mr. Tester`s Statement and was identified in Mr. Burnett`s submissions (see `Admitted Exceptions' above).

85. A second category consists of data which it was right not to disclose (either the data or its existence) when it was acquired or subsequently, but where because of the passage of time or for some other reason that is no longer the case. The simplest way of describing this category might be "old" or "time-expired files" but the situation is more complicated than that. We will summarise the evidence in a separate section under the (misleading) heading "Old files".

86. A third category arises when the existence of a file, and possibly all or part of its contents, could be disclosed without harm to national security, however long it is since the data were acquired. Requests falling within this category can only be identified if the file is examined and the appropriate decision is made in response to each individual request. The present case, the Appellant submits, is an example of this.

United States of America

87. We have explained above why we have not found it necessary to consider evidence as to the history of and justification for a NCND (or similar) policy in other States. We should, however, refer briefly to the position in the United States of America. There, the individual has a right of access to information under the Freedom of Information Acts but this right is subject to statutory exceptions. Express provision is made for cases where the existence or non-existence of data is itself classified material and is exempt from the provisions of the Act. One of the permitted exemptions is where national security would be compromised by disclosure of that fact. In such cases, a non-committal NCND response is permitted and has been approved by the Courts; indeed, it is known colloquially as the 'Glomar' response, from 'Glomar Explorer' the name of the vessel involved in a leading case (Phillippi v. CIA 546 F. 2d. 1009 (D.C.Cir. 1976); see also Gardels v. CIA (1982) 689 Fed. Rep. 2d.Ser. 1100).

88. There is extensive provision for review of the executive agency`s decision, if necessary by in camera proceedings in Court. No support can be found for a blanket exemption which relieves U.S. agencies of the duty to give individual consideration to each

request.

Old files

89. A comprehensive review of the current state of Security Service files was contained in a statement made by the Home Secretary in the House of Commons on 25 February 1998 (Hansard col. 341). He made a supplementary statement on 29 July 1998 " on the subject of the Security Service`s file holdings and on the Service`s file destruction programme"(Hansard col. 251).

90. The following is a brief summary. The Service holds about 440,000 files, of which 290,000 relate to individuals "who, at some time during the last 90 years, may have been the subject of Security Service inquiry or investigation". Of these, 230,000 files are 'closed', meaning that officers "may use them where necessary in the course of their current work, but may not make inquiries about the subjects of the files". 20,000 files relate to " individuals who may be under current investigation by the Service". About 13,000 of these 'active' files relate to United Kingdom citizens.

91. Further details of the procedures were given by the Commissioner for the Security Service (Sir Murray Stuart-Smith) in his annual Report for 1991 (Cm.1946):

> "The procedure for opening a file is strictly controlled. It may start as a temporary file, which has a maximum life of three years, when there is uncertainty whether the criteria for opening a permanent file are satisfied. These criteria have their basis in the Service's functions and require high standards of accuracy. If and when these criteria are satisfied, the permanent file will be opened. The Service then applies a system of colour coding which controls how the files are used. Once a file is opened, there is a period coded "green", during which inquiries may be made about the subject. The length of the green period varies according to the reason why the particular file was made. It may be extended as a result of the receipt of new information. At the end of the green period it changes to "amber", under which inquiries are prohibited, but any relevant information that the Service receives about the subject may be added to their file. After the designated amber period the file is coded "red". During this period, inquiries continue to be prohibited and any addition of substantive information is also prohibited. Finally, after a period of red coding, the file is microfilmed. The hard copy is destroyed and the entry for the file in the Service's central index is transferred from the Live Index to the Research Index. The research Index is usually consulted only when it is thought that old files may exist which are relevant to current work. In practice the volume of checks against the Research Index is small: for instance, it is not consulted in vetting checks."

92. In the same (1991) Report, the Commissioner also described the Service`s general policy with regard to retaining records -

> " The Service's general policy is to retain records indefinitely in case they are of relevance at any time in the future to the Service's work. In the past, espionage investigations have been seriously hampered because the Service's earlier practice had not prohibited destruction. Reconstruction of a number of files was attempted but this was not satisfactory. Since then the Service has changed its policy and, save in exceptional cases, files are retained. The Service instituted its present general policy on retention of records on the basis that they are the key to their work and they cannot accurately predict when files will ever be needed again. In my opinion as a general policy this is acceptable".

93. Another relevant aspect of this topic is the policy of the Service with regard to the destruction of records which it no longer requires to hold for the performance of its statutory duties. This too was described in the Commissioner`s 1991 Report. The Security Services Act 1989 led to the Service`s former policy being changed. Before the Act, some categories of files were destroyed, including cases where files were opened on an individual but not converted into permanent files. When the Act came into force, the view was taken that even files of this kind should be retained indefinitely, in case a complaint was made against the Service in respect of the inquiries which led to it being opened (Report paras. 22-23). The Commissioner commented -

> "It seems somewhat ironical that the Service now retain such records, which it does not require for its own purposes and which it would otherwise have destroyed. But it is plain they must do so, if they are to enable the tribunal to carry out its investigations and in appropriate cases make an order for the destruction of the records and an award of compensation. (Schedule 1 paragraph 6)".

94. Nevertheless, in his July 1998 statement to the House of Commons the Home Secretary said this -

> "It has long been the policy of the Security Service to review its file holdings and to destroy those files which it no longer requires for operational purposes and which do not merit retention on grounds of historical interest. In the period between its formation in 1909 and the early 1970s the Service destroyed well over 175,000 files. The destruction programme was then halted in response to concern that it had impeded investigations into espionage cases. In the early 1990s. following the collapse of Soviet Communism and the associated decline in the threat from subversion, the review and destruct programme was reinstated. Since then, more than 110,000 files have been destroyed or have been earmarked for destruction.

> In reviewing files for destruction, the Service takes account of their operational value, their historical significance, and the Service's obligation to retain certain categories of records against the possibility of a complaint to the Security Service Tribunal. With these criteria in mind, the Security Service continues to review its closed files for destruction and will continue to destroy files which no longer need to be retained on those grounds. The rate of review and destruction is dependent upon the resources which the Service can afford to spare for the task".

95. The Home Secretary then dealt with a further aspect, which arises because the Service is subject to the Public Records Act 1958 and therefore has a statutory duty to select certain files for preservation. Guidelines for this selection process have been agreed between the Service and the Public Records Office. One of the criteria is, of course, that the file can be released without harm to national security. Upon release to the Public Record Office, the file and its contents become public knowledge, which is the antithesis of refusing to acknowledge whether a file exists.

96. The conclusion we draw from this and other evidence is that Service files on individuals are vetted for the purposes of (1) establishing whether they should move from 'green' to 'amber' or from 'amber' to 'red' as described above; (2) deciding whether the file and its contents can be destroyed; and (3) deciding whether they can be released to the Public Record Office. There is no evidence as to whether or not a file is vetted in response to a request for its existence or its contents to be released to a person interested in them, in order to check on the national security implications of the requested release.

97. It is important to distinguish between the question whether a file can be destroyed and the question whether its existence can be acknowledged or its contents released without endangering national security. The former depends upon an assessment of its future usefulness to the Service. The latter clearly depends on quite different considerations.

Safeguards and other remedies

98. An important part of the Respondent`s case is the existence of machinery recently established by the Regulation of Investigatory Powers Act 2000 ("RIPA 2000") for "dealing with complaints by anyone aggrieved by anything which they believed the Service had done in relation to them or their property" (quoted from Mr. Tester`s Affidavit para. 7). An independent Tribunal, the Investigatory Powers Tribunal appointed under section 65 of RIPA

2000 is “the appropriate forum for any complaint” if a person is aggrieved by “conduct by or on behalf of any of the intelligence services” (section 65 sub-sections (4) and (5)).

99. The submission was stated by Mr. Tester as follows -

> “It is open to anyone who believes that the Security Service improperly holds personal data on him or her to complain to the new .....Tribunal for a full independent investigation.....the Tribunal is under a duty to hear, consider and determine any complaint within its jurisdiction unless it is frivolous or vexatious. The comprehensive nature of the Tribunal`s jurisdiction .....means that it is likely to be a more effective forum than the Data Protection Tribunal for the consideration of complaints that the Security Service (or any other intelligence agency) has acted improperly in respect of personal data processed by it.”

His evidence referred also to the role of the Intelligence Services Commissioner, also created by RIPA 2000.

100. Mr. Burnett QC developed the argument at the hearing, in the context of Mr. Nicol`s submission, which Mr Burnett accepted, that our primary concern was the Certificate and whether or not the Minister had reasonable grounds for issuing it. His contention was that the Certificate gave effect to the NCND policy, and that the validity of that policy was the only issue before us at this stage of the proceedings. If the Certificate was upheld, it would mean that the Service would have a statutory defence to any application by the Appellant under section 7(9) of the Act. But we were not concerned with the individual merits of the Appellant’s claim. Those could be considered by the Investigatory Powers Tribunal, if the Appellant believed that the Service had acted wrongly in his case, and that Tribunal would determine the substance of his complaint. The existence of this safeguard was therefore relevant, Mr. Burnett submitted, to the reasonableness or otherwise of authorising the Service to reply to section 7(1)(a) requests in NCND terms. Any individual who feels aggrieved by this has a full, fair and effective remedy elsewhere.

101. This submission underlines the fact that we were being asked, on this occasion, to determine whether the Respondent had reasonable grounds for issuing the Certificate pursuant to the NCND policy, not to consider whether the Service, not the Respondent, responded properly and lawfully to the Appellant`s individual requests. Questions arose as to whether, for example, the Service`s refusal to give a positive response could amount to “conduct” within section 65(5) of RIPA 2000, so as to bring the complaint within the

jurisdiction of the Investigatory Powers Tribunal. But these are of subsidiary importance to the main submission, which we have summarised above.

102. We add for completeness that we have considered whether Section 28(6) of the Act could be regarded as an alternative remedy. This provision on its face contemplates:-

(i) extant proceedings under or by virtue of the Act; the nature of those proceedings is otherwise unrestricted in terms of party, subject matter, forum etc;

(ii) a Ministerial certificate identifying personal data to which it applies by means of a general description of s.28(2)(3)

(iii) a claim by data controller (DC) that it applies to 'any' personal data. This must mean particular data; see the subsequent phrase "the personal data in question";

(iv) an application by any other party to the proceedings: it poses the question 'other' than whom? In relation to a s.28(4) appeal; this means the Minister SI 2000 No. 206 2(3);

(v) a ruling by the Tribunal that the certificate either does or does not apply to the PD in question.

This subsection does not comes into play here at all because while criteria (i) (ii) and (iv) may be satisfied, criteria (iii) and (v) are not. Criterion (iii) is not satisfied because it is in issue whether relevant personal data exist. s.7(1)(a) invites disclosure of whether personal data are held or not; s.7(1)(b)(c) are by contrast are premised on the existence of such data held by a data controller. Criterion (v) is equally not satisfied. The exercise contemplates the Tribunal looking at (a) the certificate (b) the personal data in question (which ex hypothesi, the Tribunal must identify) and saying that (a) does/does not cover (b)). This exercise cannot be performed when Tribunal do not have (b).

103. We say nothing about the situation which might arise, if a Minister issued a Certificate for the purposes of a specific application. The existence of alternative remedies, or safeguards, might well be relevant to the reasonableness or otherwise of issuing a Certificate of that kind, though questions would remain about the relationship between the two Tribunals which we need not answer here. The Certificate dated 22 July 2000, as we have emphasised previously, is in general terms and was intended to implement the NCND policy with prospective effect. The submission is that applicants as a class have their remedies elsewhere, in any case where information or data are wrongly withheld by the Service, and that this fact

is relevant to the question whether there were reasonable grounds for implementing the NCND policy in this way.

104. We stop short of rejecting this submission, because clearly the existence or non-existence of other safeguards for persons affected by the issue of the Certificate is potentially relevant to the question whether the Minister had reasonable grounds for issuing it. But it is a factor of limited weight in the present case. The issue essentially is whether the requirements of national security outweigh the personal rights of individuals under the Act. Those are substantial matters, and the fact that other safeguards may be available to them does not weigh heavily in the scales.

Government Procedures

105. No submissions were addressed to us as to the practical consequences for the Home Office and the Service if the 22 July 2000 Certificate is quashed, but we have thought it right to consider what these consequences might be. The Act contemplates a Certificate in general terms (as regards the data to which it applies) which is expressed to have prospective effect (section 28(3)). If the Certificate referring to all data processed by the Service pursuant to all its statutory functions is quashed, it will be because cases can arise where the claim to safeguard national security cannot be justified. We cannot say what the number of such cases might be.

106. Any revised Certificate, therefore, would have to be confined to cases where a positive form of response would prejudice national security. A Certificate could be worded accordingly, but the Service would have to decide on the proper response to each individual request. The administrative burden placed on the Service will be lightened if the obligation to consider each individual request is limited to requests which are supported by evidence sufficient to establish a prima facie case that data exists, as is the position here. We express no view as to whether or not the obligation is, or could be, limited in that way.

OVERVIEW

107. The question whether the Minister had reasonable grounds for issuing the Certificate dated 22 July 2000 arises in the context of a case where the individual has requested to be informed whether his personal data are being processed (meaning held) by the data controller: this preliminary request was made under section 7(1)(a) of the Act.

108. The Appellant was given a deliberately ambiguous reply pursuant to the NCND policy, and so the Service being the data controller has not admitted whether or not it processes personal data of which the Appellant is the data subject.

109. The reply was authorised by the Certificate, which is " conclusive evidence" that the exemption from section 7(1)(a) is required for the purpose of safeguarding national security (section 28(1) and (2)), unless it is quashed by the Tribunal.

110. We emphasize that the issue is limited in this way, because there is a fundamental difference between non-compliance with the requirements of section 7(1)(a) , where the data controller refuses to say whether or not personal data exists, and those of the remaining provisions of section 7, which require him to provide information regarding personal data which he does hold. In cases where section 7(1)(a) is relied upon, it is not conceded that relevant personal data does exist.

111. The appeal proceeds on the basis that section 7(1)(a) does apply and that the exemption given by the Certificate can have effect, notwithstanding that personal data relating to the Appellant may or may not be held. It has not been contended that our jurisdiction under section 28(4) cannot be exercised in this possibly hypothetical situation.

112. For the reasons given above, we have addressed the question whether the Minister had reasonable grounds for issuing the Certificate without particular regard to the circumstances of the present case. Both parties submitted that we should adopt this approach. The Certificate is in general terms and was intended to have prospective effect. Their submissions centred on NCND as a matter of policy - did the Minister have reasonable grounds for providing the Service with a blanket exemption from the provisions of section 7(1)(a)?

CONCLUSION

113. We have concluded that he did not. Our reasons in substance are these:-

(A) the blanket exemption given by the Certificate in relation to section 7(1)(a) is wider than is necessary to protect national security;

(B) it is common ground that some personal data relating to individuals is processed (held) by the Service which could be released to them without endangering national security;

(C) we have no evidence as to the number of requests received or likely to be received or as to the proportion of them which could lead to a decision to release personal data, if individual consideration was given to each request. We have no reason to suppose that the burden of dealing with them individually would be unduly onerous for the Service or that the proportion falling within (B) would be negligible or small;

(D) the blanket exemption relieves the Service of any obligation to give a considered answer to individual requests;

(E) we can conceive of no positive reason for giving a blanket exemption to all processing by the Service in respect of all its activities until such a time as personal data is released to the Public Record Office (if no files are destroyed, this is the effect of the evidence before us);

(F) the statutory functions of the Service, since 1989, have included matters which may, but do not necessarily overlap its task of safeguarding national security. (We bear in mind that even where personal data are acquired and held for other purposes its release (or a positive answer) to a section 7(1)(a) request could nevertheless be harmful to national security);

(G) the safeguards and other remedies available to individuals who are aggrieved by conduct of or on behalf the Service are insufficient to make reasonable the otherwise unreasonable issue of such a certificate;

(H) it has not been represented to us that it would be impossible or difficult to revise the wording of the Certificate, or to modify the internal procedures of the Service or of the Home Office so as to achieve a situation where each request is considered on its merits and either acceded to or refused accordingly. That, it

seems to us, would be a proportionate and reasonable response, given the right to respect for their private lives which individuals now enjoy;

(I) limited evidence as to the practice in other countries did not identify anywhere where an identical unchallengeable exemption was permitted. Notably the practice in the U.S.A. was more considerate of individual rights than the practice in the United Kingdom exemplified in these proceedings;

(J) the Certificate as drafted defines the exemption by reference to the purposes for which and the circumstances in which personal data is processed by the Service, rather than the consequences for national security if the data is released or even its existence is acknowledged at the time of the request.

DECISION TO QUASH

114. Mr Burnett submitted that even if we were to find that the issue of the certificate was unreasonable we should not exercise our discretion to quash it. The essence of his submission was that in order for such a remedy to be granted an appellant had to demonstrate an adverse impact of the certificate on him; and that the Appellant had failed to do so. Mr Nicol's response was that the Appellant's state of ignorance as to whether the Security Service held his personal data – the consequences of the certificate's issue and use – itself established adverse impact; and that, in any event, given the public importance of the matter at stake, we should grant the statutory remedy irrespective of the Appellant's own position.

115. We prefer Mr Nicol's submission. It seems to us that to hold a certificate to be unreasonably issued, and yet to take no steps to prevent its further use would be a recipe for confusion and further litigation. Moreover, the quashing of the certificate does not, as we have pointed out, compel The Secretary of State to accede at once to applications by data subjects under section 7 of the Act. He will have time, if he sees fit, to design and issue a certificate which conforms with our judgement.

116. We therefore quash the Certificate dated 22 July 2000 in the exercise of our powers under section 28(5) of the Act.

117. We will hear further submissions with regard to costs and any other consequential matters, when the decision is handed down at the Royal Courts of Justice on Monday 1 October at 2.30pm

Signed This 1st day October 2001

…….. The Rt. Hon. Sir Anthony Evans (President)

…… . The Hon. Michael Beloff QC

…….. Mr James Goudie QC

118. The following summary, although numbered separately, forms part of this decision.

SUMMARY OF DECISION

INFORMATION TRIBUNAL – NATIONAL SECURITY APPEALS

NORMAN BAKER MP :APPELLANT

SECRETARY OF STATE FOR THE HOME DEPARTMENT: RESPONDENT

1. The Appellant asked the Security Service to inform him whether or not it is processing his personal data and, if data exists, what such data are.

2. The request was made under section 7(1) of the Data Protection Act 1998. "Process" as defined by the Act includes "holds".

3. Subsequently, the Appellant produced evidence which, he asserts, establishes that he was the subject of investigation by the Service during the years 1985 – 1989, and that it holds a personal file on him. That evidence has not been tested, and we do not know whether it is correct.

4. The Service gave a non-committal reply to the request, consistently with its policy of answering such requests in terms which "neither confirm nor deny" that relevant data exist. The policy is known as "NCND". A positive response would state whether or not personal data were being processed (and it might go further, by releasing some or all of such data as do exist.)

5. The Service relied upon a Certificate issued by the Secretary of State for the Home Department dated 22 July 2000 as exempting it from the relevant provisions of the Act.

6. We are required by section 28(5) of the Act to determine whether the Minister had reasonable grounds for issuing the certificate. If he did not, we have power to quash the Certificate.

7. The Certificate on its true construction exempts the Service from the requirement under section 7(1)(a) of the Act to inform the Appellant whether or not his personal data are being processed by it. The Certificate, therefore, if it is valid, permitted the Service to respond with its non-committal reply.

8. The Secretary of State contended that there were reasonable grounds for authorising the Service to give a non-committal reply to this and other requests, because this was considered necessary to safeguard national security. Much of the evidence was directed towards justifying the NCND policy in relation to the operations of the Service.

9. This evidence was not challenged. The Appellant, supported by the Information Commissioner, accepted – rightly in our view – that the NCND policy is justified in relation to section 7(1)(a) requests for information made to the Service, in all cases where the Service lawfully determines that a positive response would be harmful to national security.

10. The validity of the Certificate in question was disputed, however, on the ground that its terms are wide enough to relieve the Service from any obligation to decide whether or not national security would be harmed by a positive response to the particular request. The Appellant and the Information Commissioner contended that the Minister did not have reasonable grounds for issuing the certificate in such wide terms, which could permit the Service to give the NCND reply even in cases where a positive response would not be harmful to national security.

11. The Appellant further submitted that the present is such a case, where a positive response could properly have been given to his request, but we have not found it necessary to consider his individual circumstances in this present appeal. We make no assumption as to whether or not his personal data have been acquired or are being held by the Service, and we have formed no view as to whether the existence of such data (if any) or all or part of any such data, could be disclosed to him, consistently with the Service's duty to safeguard national security.

12. Our decision in this appeal is concerned only with the duty of a data controller under

section 7(1)(a) of the Act to inform an individual by whom a request is made whether or not his personal data are being processed. We say nothing about the separate duties under different parts of section 7, including the release of all or part of data held, where considerations of national security would likewise apply.

13. We therefore have addressed the narrow issue: did the Minister have reasonable grounds for issuing the Certificate in terms which exempt the Service from the obligation to respond positively to any request made to it under section 7(1)(a) of the Act, regardless of whether or not national security would be harmed by a positive response in the particular case?

14. We have concluded, applying the principles of judicial review as they are applied by the Courts, that the Minister did not have reasonable grounds for issuing the Certificate which has this unnecessarily wide effect.

15. We do not attempt, and it is not our function, to draft the terms in which a valid Certificate might be issued. However, it seems to us that the basic defect in the certificate dated 22 July 2000 in relation to section 28(2) of the Act is that it is expressed by reference to the purposes for which and the circumstances in which personal data were acquired or are held by the Service, rather than the consequences for national security if data were released or their existence acknowledged at the time of the request.

16. We therefore, in the exercise of our discretion under section 28(5) of the Act, quash the Certificate dated 22 July 2000. This does not prevent the Secretary of State from issuing a Certificate in different terms which might be deployed in answer to the Appellant's request, whether directed specifically to that request or not, and the validity of which could be determined, if an issue arises, in separate proceedings.