IN THE INFORMATION TRIBUNAL
(NATIONAL SECURITY APPEALS PANEL)

BETWEEN:

TONY GOSLING

Appellant

and

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

DECISION

---

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 paragraph 2(1). This appeal was brought by Tony Gosling ("the Appellant") under section 28(4) of the Act.

Jurisdiction

2. The Security Service ("the Service") is a data controller who processes personal data within the scope of the Act. "Processes" includes "holds" (section 1(1)). Section 7 of the Act requires data controllers to respond to requests made by individuals for information as to whether his personal data are being processed (section 7(1)(a)) and, if they are, to have them described and communicated to him (section 7(1)(b-c)).

3. By section 28, personal data are exempt from these, and other, provisions of the Act "if the exemption from that provision is required for the purpose of safeguarding national security" (section 28(1)).

4. When a data controller fails to comply with a request made in accordance with the Act, the individual may apply to the Court for an order that he shall comply with the request (section 7(9)). An application to the Court, in a case where the data controller relies upon the national security exemption, is regulated by further provisions also contained in section 28. By section 28(2), "a certificate signed by a Minister of the Crown certifying that exemption ….. 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".

5. When an individual is "directly affected" by the Minister's Certificate, he may challenge it by appealing to this panel of the Information Tribunal, under section 28(4) of the Act. The powers of the Tribunal on such an appeal are set out in section 28(5) –

> "(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. A second branch of the jurisdiction of the Tribunal in national security cases, under section 28(6) of the Act, is not relevant to its jurisdiction in this appeal.

Background

7. By its Decision in ***Baker v. Secretary of State for the Home Department*** (1 October 2001, reported in [2001] UKHRR 1275), the Tribunal quashed a Certificate issued by the Respondent dated 22 July 2000 relating to personal data processed by the Security Service.

8. The Respondent issued a revised form of Certificate relating to personal data processed by the Service, dated 10 December 2001 (hereinafter "the Certificate").

9. The Appellant challenges the validity of the Certificate by this appeal under section 28(4) of the Act (paragraph 5 above).

The facts

10. On 26 March 2002 the Appellant wrote to the Data Controller, the Security Service, as follows:

> "I am branch secretary of the National Union of Journalists in Bristol and formally request to see my Security Service file under the Data Protection Act following the successful legal challenge of Norman Baker MP [referring to the Tribunal's Decision in ***Baker.***] I understand from the Home Office that information held by UK security services is released under "subject access" rules and the Data Protection Act. I would also appreciate any information on the "subject access" process by which I can see what information is held on me …"

11. On 5 April 2002 the Appellant submitted to the Data Controller, the Security Service, a pro forma completed form applying for access to information that might be held under the Act.

12. On 1 May 2002 someone on behalf of the Data Controller replied as follows:-

> "As previously indicated to you, under the Data Protection Act 1998, the Security Service has notified the Information Commissioner that it processes personal data for three purposes. These are: staff administration, building security CCTV and commercial agreements. The Security Service has checked its staff administration and building

security records and, subject to any further information that you might supply, holds no data about you in any of these categories. The Security Service is unable to revisit its building security CCTV footage without further details, such as date and time, of when you believe you may have been filmed. Please find enclosed a further subject access form if you wish to pursue this particular aspect of your application further, but please note that CCTV film is not normally kept for longer than one week.

Any other personal data held by the Security Service is exempt from the notification and subject access provisions of the Data Protection Act 1998 to the extent that such exemption is required for the purposes of safeguarding national security, as provided for in Section 28(1) of the Act. It has been determined that the Security Service holds no personal data to which you are entitled to have access. This response should not be taken to imply that the Security Service does or does not hold any data about you …"

13. This was a form of the non-committal NCND ("neither confirm nor deny") response, the validity of which, in appropriate cases, was not challenged in *Baker*.

14. The letter concluded "Yours sincerely ….. for Data Controller" and was subscribed only by a manuscript 'squiggle' which could not be described as a signature.

15. The Data Controller sent the Appellant a copy of the certificate signed by the Secretary of State for the Home Department on 10 December 2001, together with a copy of a document which explained the reasons for which the Secretary of State signed the certificate.

The Appeal

16. The Appellant put before the Tribunal an extensive file of materials which, he submitted, tended to raise serious concerns about the activities of the Service. Put more specifically, the Appellant submitted that the material tended to show, for example, that the Service did not keep within its proper functions, that it engaged in unlawful or unauthorised activities, that it sought improperly to exercise an influence over the media, and that it used information gathered by it for purposes beyond national security.

17. We are, of course, in no position to evaluate any of the material put forward by the Appellant, even if it were within our powers to do so, and nothing that we say in this decision should be taken to imply that we accept the Appellant's argument that the materials upon which he relies show that there are good grounds for concern about the activities of the Service. However, the Appellant quite properly did not invite us to make any specific findings in relation to the materials in question. It seemed to us, particularly from his submissions at the oral hearing, that the Appellant was saying that it was desirable that some person or body, *independent* of the Service, should check whether data held by the Service was likely to be accurate and to be used for a proper purpose. In his written submission to the Tribunal, the Appellant summarised his case in the following way:

"…If exemption from the Act is sought, under section 28, it must be up to the security service to show, *to a body trusted by MI5, the public and parliament* that a particular disclosure is likely to damage national security …

… the appointment of an *independent scrutineer* should be made transparently and in public. I suggest a nominated panel from trades unions, the information tribunal and civil liberties groups to oversea this appointment and to conduct ongoing employment reviews alongside parliamentary and public confidence in MI5's credibility whilst providing safeguards to ensure they do not abuse that trust invested in them" (paras. 18.4, 19.5, our emphasis)

18. The Respondent's Notice included "A summary of circumstances relating to the issue of the certificate and the reasons for doing so" and a copy of the Certificate dated 10 December 2001 was annexed to it. Also annexed was the document referenced DPA/S28/TSS/2 – REASONS referred to in the Certificate, paragraph 2. The Respondent's grounds were stated as follows –

> "11. The Appellant's notice of appeal raises 2 points.
>
> 12. First, the Appellant considers that, unless he challenges the certificate, he has no means of challenging whether he has been the subject of improper surveillance, whether his post has been tampered with, or whether data allegedly held by the Security Service may have compromised his Trade Union work. This is in fact a challenge to the legitimacy of the alleged processing of data by the Service, rather than a challenge to the basis upon which the certificate has been applied in this case. As such, his proper avenue of complaint is to the Investigatory Powers Tribunal. Details of how to complain to this Tribunal have already been provided to the Appellant.
>
> 13. The second point concerns the allegation that there is a blanket ban on people having access to data held by the Security Service under the Act. There is, however, no substance in this point because paragraph 2.3 of the certificate and the provisos to paragraph 3 of the certificate, read together, make it clear beyond doubt that each individual request is to be examined on its merits by the Security Service (necessarily after the time that it is received), for determination in relation to that request of the issues identified in sub-paragraphs 2.3(i) and (ii) on the merits of the case. Not all requests to the Security Service to exercise the subject access right provided by section 7(1)(a) of the Data Protection Act 1998 result in the application of the "neither confirm nor deny" policy to the entire request. In appropriate cases, the Security Service may confirm to the person making

the requests that some data is held in relation to that person, or even disclose some of that data to him.

14. Further or alternatively, the Secretary of State had reasonable grounds for issuing the certificate, which are outlined in the Reasons Document (Annex C)."

The Certificate and Reasons

19. These documents are annexed to this Decision.

20. The Certificate is expressed in general and prospective terms. The Certificate is designed to individuate the different functions of the Service and to specify the extent to which each is said to require exemption from the Data Protection Act 1998 for the purposes of safeguarding national security, in a manner that is intended to be proportionate to the perceived risk to national security if particular provisions of the Act were applied to each category of data specified in the Certificate.

21. Part A of the Certificate concerns the core intelligence gathering work of the Service pursuant to its statutory functions. Part A confers most of the exemptions provided for by section 28 of the Act, with the principal exception of the third, fourth, fifth and seventh data protection principles. The fourth data protection principle is that "personal data shall be accurate and, when necessary, kept up to date" – Schedule 1 part 1 para. 4 of the Act. Part B confers more limited exemptions for data processing carried out by other data controllers for or on behalf of the Service in relation to the Service's statutory functions. Part C confers even more limited exemptions (principally from the enforcement and data dissemination provisions) for three kinds of data: non-security related personnel records, CCTV coverage of Thames House and commercial agreements. Part D confers certain exemptions for security-related parts of personnel records which contain more sensitive information.

22. Most importantly, in the light of the decision in *Baker*, the Certificate sets out the circumstances in which the exemptions referred to above will not be claimed. Paragraph 3 of the Certificate makes the following provisos:

"(i) no data shall be exempt from the provisions of section 7(1)(a) of the Data Protection Act 1998 if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that adherence to the principle of neither confirming nor denying whether the Security Service holds data about an individual is not required for the purpose of safeguarding national security;

(ii) no data shall be exempt from the provisions of section 7(1)(b),(c) or (d) of the Data Protection Act if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that non-communication of such data or any description of such data is not required for the purpose of safeguarding national security."

23. The effect of the Certificate is, therefore, to establish a two-stage or, in certain instances, a three-stage procedure. First, the Service must identify the nature of the data requested in order to determine which part (Part A,B,C or D) of the Certificate applies and the extent of the exemption conferred in respect of that part. Secondly, if it appears that a relevant exemption in principle covers the data requested, the Service must decide whether for the purpose of safeguarding national security it should invoke for the particular request the general NCND response. Thirdly, if the Service were to decide exceptionally that the general NCND response was *not* necessary to safeguard national security in the particular case, the Service would have to determine whether it was necessary for that purpose not to communicate specific data, if any, subject to the request or data of a general description falling within the scope of the request.

The Reasons

24. The Reasons are summarised in the Certificate, as follows:

"2.1 The work of the security and intelligence agencies of the Crown requires secrecy.

2.2 The general principle of neither confirming nor denying whether the Security Service possesses data about an individual …… is an essential part of that secrecy.

2.3 In dealing with subject access requests under [the Act], the Security Service will examine each individual request to determine:

(i) whether adherence to that general principle is required for the purpose of safeguarding national security, and

(ii) in the event that such adherence is not required, whether and to what extent the non-communication of any data or any description of data is required for the purpose of safeguarding national security.

2.4 ……."

25. The Reasons also include the following –

"5. The need for and use of the "neither confirm nor deny" policy

5.1 ….. Put simply, the policy is a way to preserve the secrecy described above by giving a vague and non-committal answer.

5.3 ….. To ask whether the Security Service holds personal data on an individual often amounts to asking whether there is or has been an investigation.

5.4 ….. By logical extension, the policy must apply even if no investigation has taken place. If the Security Service said that it did not hold information on a particular person, inevitably over time those on whom it did not hold information would be able incrementally to deduce that fact ……

5.5 If individuals intent on damaging national security could confirm that they were not the subjects of interest to the Security Service, then they could undertake their activities with increased confidence and vigour …..

5.6 Conversely, confirmation to individuals that they are subjects of interest may create or fuel suspicions that associates of theirs are assisting the Security Service ….."

6. The Safeguards and statutory controls that exist on the activities of the Security Service

6.1.1 Legal constraints placed on the Security Service and its work ….. by Parliament through:

iii the Regulation of Investigatory Powers Act 2000. This law governs the interception of communications, the carrying out of surveillance and the use of "covert human intelligence sources" eg undercover officers or agents.

6.1.9 The Regulation of Investigatory Powers Act 2000 also set up the Investigatory Powers Tribunal ….

7. Non-Data-Protection-Act Remedies

7.1 Anyone who feels aggrieved by anything which he or she believes the Security Service has done in relation to them or their property may complain to the independent Investigatory Powers Tribunal ……. There is no bar to what Tribunal members can see when looking into a complaint ……"

8. The test that should be used to balance the need to safeguard national security and purposes of the Data Protection Act 1998

8.2 ….. the Home Secretary has balanced the need to safeguard national security against the purposes and entitlements conferred by the DPA ……."

Evidence

26. The Respondent relied on (1) a Witness Statement by A.J. Tester, a civil servant of the Home Office, who produced the Witness Statement, with enclosures, that he made in connection with the *Baker* appeal, and confirmed that the Security Service asked the Home Secretary to sign a new certificate "whose terms took account of that decision" (2) a witness statement made by an unnamed Security Service witness which had been relied on in *Baker* and (3) a further statement by an unnamed Security Service witness, who described the operational duties and needs of the Service and justified the "neither confirm nor deny" policy adopted by it. He also produced evidence of corresponding laws and practices in other jurisdictions.

Hearing

27. The hearing of the appeal took place on 31 January 2003. No application was made by the Appellant that the hearing should take place in public, pursuant to rule 23(1) of the Data Protection Tribunal (National Security Appeals) Rules 2000. However, subsequently on 4 March 2003 the Tribunal directed that the hearing of the appeal in the case of Mr Hitchens should take place in public, and the Tribunal thought it right in those circumstances to give the Appellant retrospectively the opportunity to have the hearing in his appeal treated as having taken place in public. The Appellant did so apply and the Respondent consented to the application. The Tribunal accordingly directed that the hearing should be treated as having taken place in public.

Conclusions

28. It can be seen that the Appellant's case is specific and focused. He does not challenge the reasons for the issue of the Certificate (as set out in the document referred to at paragraph 18); and, in particular, he does not challenge the reasons for the general NCND policy. Nor does he contend that the Minister had in law no power to issue a certificate which in effect delegated to the data controller concerned the decision whether or not the

policy of NCND should be applied in any particular case. No party to the current appeals has advanced such a contention, and it would not be appropriate for the Tribunal to say anything further about such a possible argument. Rather, the Appellant challenges the reasonableness of delegating the power to the Service, namely, a procedure by which the *Service alone* determines, firstly, whether the policy should apply in a particular case, and, secondly, whether, even if it should not, specific data or data of a general description should be communicated to a person making a request for access. (see paragraphs 22 and 23 above).

29. We see force in the central point made by the Appellant. Section 7 of the Act creates a general entitlement for an individual to ask and be told by anyone who decides on purposes of processing personal data whether personal data on that individual is being processed, which includes being held, and, if it is, be told certain information about that data. The main rationale for subject access is that an individual can satisfy himself or herself as to what, if any, relevant personal data is being processed, that any processing is done for a proper purpose, that the data is accurate, and to whom the data may be disclosed. If dissatisfied with the outcome of the request, the individual can then take corrective action.

30. On any view the NCND policy creates a major inroad into what would otherwise be the right of the individual to obtain access to personal data for the purposes referred to above. Assuming that the general NCND policy is itself justified – a premise, as we observed, not challenged by the Appellant – the Service accepts that the policy is not absolute. As explained by the Service witness (see paragraph 26 above), an individual may have "conclusive proof" that personal data is held on him or her because, for example, Service Officers have given evidence concerning the applicant (perhaps in criminal cases or proceedings before the Special Immigration Appeals Commission). Similarly, current and former employees by virtue of the special knowledge gained as a result of their employment, will know about the existence of a file on them that relates to sensitive security matters. However, it appears to us that an issue might well arise, for example, as to whether the particular applicant did

in fact have "conclusive proof" that the Service held personal data on the applicant; or as to whether in relation to a former employee the personal data identified by the Service was reasonable in scope, having regard to the need to safeguard national security. There may be other, as yet not specifically identified cases, where departure from NCND might be justifiable. In all such cases the Service itself would, under the provisos in the certificate, exclusively decide the issue.

31. In those instances where the Service thought it appropriate to depart from the NCND policy, a decision would also need to be taken as to whether no access should be given to any relevant personal data on the grounds that communication of the specific data or of data of the general description subject to the request would put national security at risk. Although, as we said above, we have no grounds for believing that the Service conducts itself otherwise than efficiently and lawfully, it would be naïve to rule out the possibility that data might not be communicated, not because communication might pose a real and significant threat to national security, but because it might raise questions about the activities of the Service. Again, under the provisos in the certificate, it is the Service alone which makes the decision.

32. The question, therefore, arises for us whether, applying judicial review principles it was lawful for the respondent by the Certificate to leave the application of the NCND policy exclusively in the hands of the Service. We had no evidence before us that the respondent had specifically considered whether, consistently with the needs of national security, the application of the NCND policy to at least certain cases might not involve some independent check so that the procedure would arguably be more transparent and possibly inspire greater public confidence in the result. However, Mr. Tam, on behalf of the respondent, made submissions that the present procedure laid down in the certificate was lawful, accepting, for the purposes of this appeal, that the respondent might lawfully have adopted a *different* procedure if he had deemed it appropriate, balancing the need to safeguard national security against the other considerations which we have mentioned.

(a) Delegation to the Security Services.

33. Mr. Tam pressed the following argument upon us. He submitted that the Service was best placed, through its experience and expertise, to make the relevant decisions. It is true that the courts in the United Kingdom have traditionally accorded a high degree of deference to the executive on matters affecting national security, the high water mark perhaps being the *Zamora* [1916] 2 AC 77, where Lord Parker said:

> "Those who are responsible for the national security must be the sole judge of what the national security requires. It would be obviously undesirable that such matters should be made the subject of evidence in a court of law or otherwise discussed in public"

34. The *Zamora* was cited in *Council of Civil Service Unions v Minister for the Civil Service* [1985] 1 AC 374 ("CCSU") where Lord Scarman put the matter as follows:-

> "The point of principle in the appeal is as to the duty of the court when in proceedings properly brought before it a question arises as to what is required in the interest of national security. The question may arise in ordinary litigation between private persons as to their private rights and obligations: and it can arise, as in this case, in proceedings for judicial review of a decision by a public authority. The question can take one of several forms. It may be a question of fact which Parliament has left to the court to determine: see for an example section 10 of the Contempt of Court Act 1981. It may arise for consideration as a factor in the exercise of an executive discretionary power. But, however it arises, it is a matter to be considered by the court in the circumstances and context of the case. Though there are limits dictated by law and common sense which the court must observe in dealing with the question, the court does not abdicate its judicial function. If the question arises as a factor to be considered in reviewing the exercise of discretionary power, evidence is also needed so that the court may determine whether it should intervene to correct excess or abuse of the power…….

My Lords, I conclude, therefore, that where a question as to the interest of national security arises in judicial proceedings the court has to act on evidence. In some cases a judge or jury is required by law to be satisfied that the interest is proved to exist: in others, the interest is a factor to be considered in the review of the exercise of an executive discretionary power. Once the factual basis is established by evidence so that the court is satisfied that the interest of national security is a relevant factor to be considered in the determination of the case, the court will accept the opinion of the Crown or its responsible officer as to what is required to meet it, unless it is possible to show that the opinion was one which no reasonable minister advising the Crown could in the circumstances reasonably have held. There is no abdication of the judicial function, but there is a common sense limitation recognised by the judges as to what is justiciable: and the limitation is entirely consistent with the general development of the modern case law of judicial review." (404 EG, 406 GH – 407A)

35. In *CCSU* Lord Diplock stated his view trenchantly:

"National security is the responsibility of the executive government, what action is needed to protect its interests is, as the cases cited by my learned friend, Lord Roskill, establish and common sense itself dictates, a matter upon which those upon whom the responsibility rests, and not the courts of justice, must have the last word. It is par excellence a non-justiciable question. The judicial process is totally inept to deal with the sort of problems which it involves" (at 412 EF); see also Lord Fraser at 410G – 403B; Lord Roskill at 420B – 421G.

36. The reluctance of the courts to "second guess" the executive when questions of national security have been in issue has been a feature in more recent cases. In *R v. Secretary of State for the Home Department, ex parte Cheblak* [1991] 1 WLR 890 the applicant challenged a notice of intended deportation given by the Home Secretary on the grounds that his deportation "would be conducive

to the public good for reasons of national security". The Home Office stated that the applicant's known links with an organisation which it was believed could take terrorist action against Western targets in support of the Iraqi regime made his presence in the United Kingdom an unacceptable security risk; and an affidavit sworn on behalf of the Home Secretary stated that further details could not be disclosed because it would be an unacceptable risk to national security to do so.

37. Lord Donaldson MR, in rejecting the application, said:

" … the exercise of the jurisdiction of the courts in cases involving national security is necessarily restricted, not by an unwillingness to act in protection of the rights of individuals or any lack of independence of the Executive, but by the nature of the subject matter. National security is the exclusive responsibility of the Executive and, as Lord Diplock said in *CCSU*: "It is par excellence a non-justiciable question"" (at 902 gh); see also Beldam L.J. at 912d ("the statement that to give further information might jeopardize national security is one that the court is bound to accept") and Nolan L.J. at 916b ("the practical result …. Is that the Secretary of State acting in good faith, is effectively protected not only from the risk of appeal, but from the risk of a writ of habeas corpus".

38. Similarly, in *R v. Secretary of State for the Home Department ex p. Chahal* [1995] 1 WLR 526 the Home Secretary served a deportation notice on the applicant which stated that for reasons of a political nature, namely the international fight against terrorism, his continued presence in the United Kingdom would not be conducive to the public good. During the course of his judgment Staughton L.J. said:

"But we cannot determine whether the Secretary of State was right, after the report of the advisory panel, to reach those conclusions. Nor can we review the evidence. That was explained by Dillon L.J. in *NHS v. Secretary of State for the Home Department* [1998] Imm AR 389 at 395 and by Geoffrey Lane L.J. in *R v. Secretary of State for the Home Department ex p. Hosenball*

[1977] I WLR 766 at 783. We have to accept that the evidence justifies those conclusions" (at 531 ef) and later:

"… we do not have the evidence on which the Secretary of State considers him a risk to national security, for the reasons already indicated. So we cannot balance the threat [sc. to the applicant's life] on the one hand against the risk on the other" (at 535 d); cf Neill L.J. at 543 d ("the court has the right to scrutinise a claim that a person should be deported in the interests of national security but in practice this scrutiny may be defective or incomplete if all the relevant facts are not before the Court") and at 545 b ("on the facts of this case the grounds of national security relied on by the Secretary of State cannot be challenged").

39. In a somewhat different context in *R v. Secretary of State for the Home Department, ex parte McQuillan* [1995] 4 All ER 400 the applicant challenged exclusion orders against him under section 5 of the Prevention of Terrorism (Temporary Provisions) Act 1989 prohibiting him from being in or entering Great Britain on the ground that he was or had been involved in acts of terrorism. An assistant secretary of the Home Office deposed that it was not possible for the applicant, nor was it ever possible for any person against whom such an order was made, to be informed in greater detail of the reasons why the order had been made. Sedley J. was clearly troubled by the lack of judicial control but felt constrained by authority to hold that national security was sufficient to preclude any inquiry by the court into the rationality of the decision and the decision had to be accepted by the court without further scrutiny.

40. This traditional approach of the United Kingdom courts has not, however, met complete approval from the European Court of Human Rights or the Court of Justice of the European Union. *Chahal* (see paragraph 38 above) found its way to Strasbourg (*Chahal v. United Kingdom* (1997) 23 E.H.R.R. 413), and the European Court of Human Rights found a violation of Article 5(4) of the Convention. The Court recalled that because national security was involved, the domestic courts were not in a position to review whether the decisions to

detain the applicant and to keep him in detention were justified on national security grounds (paragraph 130). In an important passage the Court said:

"The Court recognises that the use of confidential material may be unavoidable where national security is at stake. This does not mean, however, that the national authorities can be free from effective control by the domestic courts whenever they choose to assert that national security and terrorism are involved. The court attaches significance to the fact that … in Canada a more effective form of judicial control has been developed in cases of this type. This example illustrates that *there are techniques which can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice* (paragraph 131, our emphasis).

41. The Court repeated this formulation in *Tinnelly & Sons Ltd v. United Kingdom* (1999) 27 E.H.R.R. 249 where the applicant alleged unlawful religious discrimination in the allocation of a public contract and was met by a conclusive ministerial certificate under section 42 of the Fair Employment (Northern Ireland) Act 1976 that the decision not to grant the applicant the contract in question was an act done for the purpose of safeguarding national security or the protection of public safety or order.

42. The Court in *Tinnelly* continued as follows:

"The introduction of a procedure, regardless of the framework used, which would allow an adjudicator or tribunal fully satisfying the Article 6(1) requirements of independence and impartiality to examine in complete cognizance of all relevant evidence, documentary or other, the merits of the submissions of both sides, may indeed serve to enhance public confidence. The Court observes in addition that McCollum J. [the judge in Northern Ireland] was unable under the present arrangements to dispel his own doubts about certain disturbing features of the Tinnelly case since he, like Tinnelly and the Fair Employment Agency, was precluded from having cognizance of all relevant material in the possession of NIE, the respondent in the

proceedings instituted by Tinnelly under the 1976 Act. This situation cannot be said to be conductive to public confidence in the administration of justice" (paragraph 78).

43. In European Community law the most notable case remains *Johnston v. Chief Constable of the Royal Ulster Constabulary* (Case 222/84) [1986] ECR 1651 where the applicant, a former woman member of the RUC Reserve, alleged unlawful sexual discrimination and was met by a conclusive ministerial certificate that the act of refusing to offer the applicant further employment in the RUC Reserve was done for the purpose of safeguarding national security and protecting public safety and public order. As to the certificate, the Court of Justice held:

"19. By virtue of Art 6 of Directive 76/207 [the equal treatment Directive], interpreted in the light of the general principle stated above, all persons have the right to obtain an effective remedy in a competent court against measures which they consider to be contrary to the principle of equal treatment for men and women laid down in the directive. It is for the member states to ensure effective judicial control as regards compliance with the applicable provisions of Community law and of national legislation intended to give effect to the rights for which the directive provides.

20. A provision which, like Art 53(2) of the 1976 order, requires a certificate such as the one in question in the present case to be treated as conclusive evidence that the conditions for derogating from the principle of equal treatment are fulfilled allows the competent authority to deprive an individual of the possibility of asserting by judicial process the rights conferred by the directive. Such a provision is therefore contrary to the principle of effective judicial control laid down in Art 6 of the directive" (see also *R v. Secretary of State for the Home Department, ex parte Gallagher* [1996] 1 C.M.L.R. 557, in contrast to *McQuillan* above).

44. We are fully conscious of the different contexts in which *Chahal, Tinnelly* and *Johnston* were decided. *Chahal* concerned the right not to be unlawfully

detained in custody, and *Tinnelly* and *Johnston* concerned the right not to be discriminated against on sexual or religious grounds. However, we discern in the European jurisprudence a broader principle to the effect that claims to national security should, save perhaps in the most exceptional and extreme circumstances, be subject to *some* process of independent scrutiny, even if that process cannot perforce be as intense as might be expected in other situations, and even if a high degree of deference must continue properly to be accorded to the judgment of the executive, particularly to those within the executive who have long experience and unrivalled expertise in what is arguably the most delicate function of government. This principle is underpinned by the need in a modern democratic society to give fair and proportionate weight to the protected rights or interests of individuals (whether in freedom of person, rights against impermissible discrimination or rights to private life), even in situations where issues of national security are in play; and the principle is also supported by the aim of promoting public confidence in the results that are produced by the chosen procedures.

45. We observe also that Parliament responded to *Chahal* by enacting the Special Immigration Appeals Commission Act 1997 which established the Special Immigration Appeals Commission with jurisdiction in cases where the Home Secretary decides to deport a person in the public interest and on national security grounds. The working of the Special Immigration Appeals Commission shows that a form of independent scrutiny is feasible even in relation to national security.

46. It might be objected that any independent checking of the application to a particular case of the certificate which we are considering could lead to such an intense scrutiny that it would itself be detrimental to national security. We do not find such an objection convincing, particularly in the light of the authoritative guidance recently given by the House of Lords on the role appropriate to an independent body assessing claims to national security: *Secretary of State for the Home Department v. Rehman* [2001] 3 WLR 877

47. In the words of Lord Hoffman:

"This brings me to the limitations in the appellate process. First, the commission is not the primary decision-maker. Not only is the decision entrusted to the Home Secretary but he also has the advantage of a wide range of advice from people with day-to-day involvement in security matters which the commission, despite its specialist membership, cannot match. Secondly, as I have just been saying, the question at issue in this case does not involve a Yes or No answer as to whether it is more likely than not that someone has done something but an evaluation of risk. In such questions an appellate body traditionally allows a considerable margin to the primary decision-maker. Even if the appellate body prefers a different view, it should not ordinarily interfere with a case in which it considers that the view of the Home Secretary is one which could reasonably be entertained. Such restraint may not be necessary in relation to every issue which the commission has to decide …. But I think it is required in relation to the question of whether a deportation is in the interests of national security ….

…. The need for restraint flows from a commonsense recognition of the nature of the issue and the differences in the decision-making process and responsibilities of the Home Secretary and the commission" (at 896). See also Lord Slynn at 886; Lord Steyn at 889, and the application of these principles in *A v. Secretary of State for the Home Department* (2003) 2 WLR 564, especially per Lord Woolf CJ at para. 40 and Brooke L.J. at paras. 66-81.

48. In the light of the European jurisprudence to which we have referred, and the Parliamentary response to *Chahal*, we have serious doubts whether Parliament could have intended that the Service itself would exclusively, without *any* form of independent scrutiny, determine the application to particular cases of the NCND policy in the kind of circumstances that we have described at paras 30 and 31 above. That doubt is strengthened when we bear in mind the powerful European dimension to the Act which we explained in *Baker* (see, in particular, paragraphs 50-64): the Act gives effect to the European Community Data Protection Directive, made by the European Parliament and the Council on 24 October 1995, and that Directive in turn gives substance and amplifies *inter alia* the rights recognised in Art 8 (respect for private life) of the 1950

Convention, now of course given further effect to in UK law by the Human Rights Act 1998.

(b) The Investigatory Powers Tribunal

49. During the course of his submissions Mr. Tam referred to the powers of the Investigatory Powers Tribunal (established under section 65 of the Regulation of Investigatory Powers Act 2000, "RIPA"). The Investigatory Powers Tribunal deals with a wide range of complaints that may be made about the exercise of powers under RIPA. Tribunals of this kind were previously established under the Interception of Communications Act 1985, the Security Service Act 1989 and the Intelligence Services Act 1994. These different tribunals are now combined into a single tribunal, with Lord Justice Mummery as its current president. The tribunal is the appropriate forum for dealing with complaints concerned with "conduct" by the intelligence services which relate to the complainant, his or her property or his or her communications.

50. In the light of our concerns in respect of the exclusive decision-making power conferred on the Service by the provisos in the certificate, we asked Mr. Tam whether the respondent accepted that the Investigatory Powers Tribunal had jurisdiction to consider any complaint which an individual might wish to make about the giving to him by the Service of an NCND response to a data subject access request made by him. At the hearing Mr. Tam was unable either to confirm or deny whether the respondent did so accept. However, in a subsequent note he made clear the position of the respondent, as follows:-

"The Investigatory Powers Tribunal does have jurisdiction to consider any such complaint. Depending on the terms of the complaint to the Investigatory Powers Tribunal, such jurisdiction will arise under one or other, or both, of the following provisions:-

(a) section 65(2)(b) and 65(4) of the 2000 Act, in that the giving of an NCND response by the Security Service is conduct in relation to that person, and the Tribunal has jurisdiction to consider a complaint by that person if he is aggrieved by such conduct; and

(b) section 65(2)(a) of the 2000 Act, in that the giving of an NCND response by the Security Service is an act of a public authority which would be unlawful under section 6(1) of the Human Rights Act 1998 if it is incompatible with a Convention right, and the Tribunal is the only appropriate forum in which a person who claims to be a victim of any unlawful act may bring proceedings against the Security Service to make such a claim."

51. Jurisdiction cannot, of course, be conferred on the Investigatory Powers Tribunal by agreement or by concession made by the Security Services, let alone the respondent to this appeal. We must, therefore, reach a view as to whether Mr. Tam's interpretation of section 65 on behalf of the respondent is sustainable.

52. Looking at section 65(5)(a), it would appear at first sight that the unqualified expression "conduct" is wide enough to include conduct of the Security Services in handling requests for personal data under the Act, particularly as section 65(5)(b) – (c) continue by describing more specifically types of conduct that are subject to earlier provisions of RIPA. However, applying general principles of statutory interpretation "conduct" has to be interpreted in the light of the purposes of RIPA. These purposes are accurately set out in the long title as:

"To make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed …"

53. This description would suggest that "conduct" for the purpose of RIPA has a narrower scope and relates to the matters specifically regulated by RIPA. The "surveillance" falling within Part II of RIPA and hence caught by section 65(5)(b) would appear not to include all forms of surveillance; and it may be that the expression "conduct" in section 65(5)(a) is simply intended to ensure that *all* forms of *surveillance* may be made the subject of complaint and of adjudication by the Investigatory Powers Tribunal. On this view, "conduct" in this respect must relate to activities of "surveillance".

54. However, even if this narrower construction of "conduct" were correct, and quite apart from the other activities included in the long title, "surveillance" – a matter falling within the scope of RIPA, as the long title shows – is itself fairly widely described in section 48(2) as including:

"(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) *recording anything monitored, observed or listened to* in the course of surveillance;" (our emphasis)

55. A person seeking personal information from the Security Services could well do so either to discover in the first instance whether he had been the subject of "surveillance", as broadly understood; or, if he believed that he had been the subject of such surveillance, to discover what had been recorded about him. An NCND answer to a request would, therefore, appear, even if somewhat indirectly, to touch on conduct relating to surveillance; and, even on a narrow construction of "conduct", the giving of an NCND response would appear to fall within section 65(5)(a). Furthermore, a person confronted with a NCND response may well be in a position to frame proceedings against the Security Services that the action is not compatible with, for example, Article 8 of the Convention. Such proceedings would then fall within section 65(2)(a).

56. Therefore we conclude that the Investigatory Powers Tribunal does have the jurisdiction which Mr. Tam accepted. Furthermore, we believe that the

Investigatory Powers Tribunal is the body best placed to determine any specific complaint that the Service has applied the provisos to the certificate in a manner that is manifestly unjustified. That Tribunal is presided over by a distinguished senior judge and has the appropriate expertise to investigate a complaint of this nature. In terms of the European jurisprudence to which we have referred, the Tribunal is independent and has the authority to call for evidence and explanation even in matters affecting national security, within the guidelines now laid down by the House of Lords in *Rehman*. However, we reiterate that, in the absence of the jurisdiction now conceded by the respondent, we would have had reservations as to whether the procedure contemplated by the provisos to the certificate accorded with the important principle which we have discerned from the European jurisprudence and which we believe is applicable to the present statutory context.

(b) Re: Ewing

57. For the sake of completion we should add that Mr. Tam drew our attention to *Re: Terence Patrick Ewing* (judgment of 20 December 2002, unreported) in which Davis J., in the context of an application to the High Court by a "vexatious litigant" for leave to appeal to this Tribunal, concluded that there were no arguable grounds for holding that the certificate of 10 December 2001 was unlawful (see, in particular, paragraphs 60-65). The applicant in that case did not advance the point that has concerned us in this appeal, and Davis J., was not therefore called upon to deal with it. We believe, therefore, that we should deal fully with the point, as we have done, rather than treating ourselves as bound by the conclusion that he reached in the absence of submissions on the relevant issue.

58. For these reasons, we dismiss the appeal.

Further Comment

59. In this case, as in *Hitchens,* the Appellant rightly complains that the letter of response from the Security Services was effectively unsigned. It was subscribed by a "squiggle" which does not identify the writer and which cannot, in our view, be regarded as a signature.

60. This unfortunate factor does not appear to be relevant to the present appeal, but it should not go unrecorded.

Signed:

SIR ANTHONY EVANS PC

ROBIN PURCHAS QC

KENNETH PARKER QC

01 August 2003

IN THE INFORMATION TRIBUNAL

(NATIONAL SECURITY APPEALS PANEL)

BETWEEN:

TONY GOSLING

Appellant

and

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

DECISION

Annex A

Certificate and ‘Reasons Document’ issued by the Secretary of State for the Home Department on 10 December 2001

ANNEX A

Certificate reference:- DPA/s28/TSS/2

SECTION 28 DATA PROTECTION ACT 1998

CERTIFICATE OF THE SECRETARY OF STATE

---

1. Whereas:

(i) by section 28(1) of the Data Protection Act 1998 ("the Act ") it is provided that 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

of the Act if the exemption from that provision is required for the purpose of safeguarding national security;

(ii) by subsection 28(2) it is provided that a certificate signed by a Minister of the Crown certifying that the exemption from all or any of the provisions mentioned in subsection 28(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;

(iii) by subsection 28(3), it is provided that a certificate under subsection 28(2) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.

2. And considering the potentially serious adverse repercussions for the national security of the United Kingdom if the exemptions hereafter identified were not available.

And for the reasons set out in document referenced **DPA/S28/TSS/2-REASONS**, in summary that:

2.1 The work of the security and intelligence agencies of the Crown requires secrecy.

2.2 The general principle of neither confirming nor denying whether the Security Service processes data about an individual, or whether others are processing personal data for, on behalf of with a view to assist or in relation to the functions of the Security Service, is an essential part of that secrecy.

2.3 In dealing with subject access requests under the Data Protection Act 1998, the Security Service will examine each individual request to determine:

i) whether adherence to that general principle is required for the purpose of safeguarding national security; and

ii) in the event that such adherence is not required, whether and to what extent the non-communication of any data or any description of data is required for the purpose of safeguarding national security.

2.4 The very nature of the work of the Security Service requires exemption on national security grounds from those parts of the Act that would prevent it, for example, passing data outside the European Economic Area and that would allow access to the Security Service's premises by third parties.

3. Now, therefore, I, the Right Honourable David Blunkett MP, being a Minister of the Crown who is a member of the Cabinet, in exercise of the powers conferred by the said section 28(2) do issue this certificate and certify as follows:-

3.1 that any personal data that are 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;

3.2 that any personal data that are processed by any other person or body (in circumstances where that data processing comprises or includes the retention or disclosure of data by that other person or body for or to the Security Service) in the course of data processing operations carried out for, on behalf of or at the request of the Security Service or in relation to the functions of the Security Service of the Security Service Act 1989 as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act that are set out in Column 2 of Part B;

3.3 that any personal data that are processed by any other person or body (other than a government department, agency or non-departmental public body) in the course of data processing operations following the data's disclosure to that person or body by the Security Service in accordance with section 2(2)(a) of the Security Service Act 1989 as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act that are set out in Column 2 of Part B;

3.4. that any personal data that are processed by the Security Service for the purposes set out in Column 1 of Part C 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 C below; and

3.5. that any personal data that are processed by the Security Service as described in Column 1 of Part D of 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 D below

all for the purpose of safeguarding national security, provided that:

(i) no data shall be exempt from the provisions of section 7(1)(a) of the Data Protection Act 1998 if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that adherence to the principle of neither confirming nor denying whether the Security Service holds data about an individual is not required for the purpose of safeguarding national security;

(ii) no data shall be exempt from the provisions of section 7(1)(b), (c) or (d) of the Data Protection Act 1998 if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that non-communication of such data or any description of such data is not required for the purpose of safeguarding national security.

4. This certificate gives notice that I require the Security Service, by virtue of my authority arising from s1(1) of the Security Service Act 1989, to report to me on the operation of the exemptions described in this certificate

PART A

Column 1	Column 2
Personal data processing in performance of the functions of the Security Service described in Section 1 of the Security Service Act 1989 as amended by the Security Service Act 1996, including recruitment of staff of the Security Service and assisting with the recruitment of staff of the Secret Intelligence Service and GCHQ and vetting of the Security Service's candidates, staff, contractors, agents and others in accordance with the government's vetting policy	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(1)(c), 16(1)(d), 16(1)(e), 16(1)(f), 17, 21, 22, and 24 of Part III; (iii) Part V; (iv) the first data protection principle; (v) the second data protection principle; (vi) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and (vi) the eighth data protection principle.

Part B

Column 1	Column 2
Personal data processing for, on behalf of or at the request of the Security Service or in relation to the functions of the Security Service described in section 1 of the Security Service Act 1989 as amended by the Security Service Act 1996 or following the data's disclosure to that person or body by the Security Service in accordance with section 2(2)(a) of the Security Service Act 1989, including recruitment of staff of the Security Service and assisting with the recruitment of staff of the Secret Intelligence Service and GCHQ and vetting of the Security Service's candidates, staff, contractors, agents and others in accordance with the government's vetting policy	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(1)(c), 16(1)(d), 16(1)(e), 16(1)(f), 17, 21, 22, and 24 of Part III to the extent that those provisions require any reference to the Security Service or data processing operations carried out by or in support of the Security Service or in consequence of a lawful disclosure by the Security Service ; (iii) Part V; (iv) section 55; (v) the first data protection principle; (vi) the second data protection principle; and (vii) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate.

PART C	
Column 1	**Column 2**
1. Personal data processed by the Security Service for the purposes of administration of human resources (including data relating to former members of staff but excluding the contents of the filing system containing confidential data as described in Part D of this table) and staff pay, tax and national insurance contributions	1. Sections 16 (1) (f), 47 and 50 and Schedule 9.
2. Personal data processed by the Security Service for the purposes of maintaining CCTV coverage of Thames House, 12 Millbank, London in relation to the security and integrity of the building	2. Sections 47 and 50 and Schedule 9.
3. Personal data processed by the Security Service for the purpose of commercial agreements (whether concluded or otherwise) or other arrangements with 3rd parties, in relation to which the Security Service supplies goods or services or under which the Security Service receives goods or services, whether the goods or services are supplied or received under those agreements, arrangements or otherwise (and to the extent that the data do not comprise data to which Parts A or B of this certificate apply)	3. Sections 16 (1) (f), 47 and 50 and Schedule 9

Part D	
Column 1	**Column 2**
Personal data processed by the Security Service for the purpose of maintaining and consulting a filing system containing confidential data about current and former members of its staff, the purpose of which is to provide personnel officers and managers with information considered necessary to make informed decisions as to the suitability of individuals for any task, appointment, posting or any other matter, with particular regard to the security implications of those decisions	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(c), 16(e), 16(f), 17, 21, 22, and 24 of Part III; (iii) Part V; and (iv) The eighth data protection principle

……[as signed]……..
The Right Hon. David Blunkett, MP

……
Dated

I confirm that the Home Secretary approved this certificate and it was signed with his personal stamp.

Name …….

Signed …….

Dated **…….**

Annex C

Document Reference **DPA/S28/TSS/2-REASONS**

REASONS FOR THE HOME SECRETARY SIGNING THE DATA PROTECTION ACT 1998 s28 (NATIONAL SECURITY) EXEMPTION CERTIFICATE COVERING PERSONAL DATA PROCESSED BY THE SECURITY SERVICE – REFERENCE DPA/S28/TSS/2

1. Introduction

1.1. The section 28 certificate, document reference **DPA/S28/TSS/2,** was signed by the Home Secretary following a request made to him by the Security Service. This document explains the reasons he did so. It is made public to allay concerns that anyone may have about the use by the Security Service of the data protection national security exemption that exists under section 28 of the Data Protection Act 1998.

1.2. Before signing the certificate the Home Secretary considered the following factors:

i. The Data Protection Act 1998 (DPA), its national security exemptions, and role of the National Security Panel of the Information Tribunal (the "Tribunal").

ii. The functions of the Security Service and its primary role in the protection of national security.

iii. Why secrecy is essential to the work of the Security Service and the damage or potential damage that can be done to national security when secrecy is compromised.

iv. The need and use of the neither-confirm-nor-deny policy.

v. The Tribunal determination in the appeal by Norman Baker MP against a s28 certificate signed by the previous Home Secretary covering personal data that the Security Service may have processed.

vi. The safeguards and statutory controls that exist on the activities of the Security Service.

vii. The non-DPA remedies open to anyone who feels aggrieved by anything which he or she believes the Service has done in relation to them or their property.

viii. The test that should be used to balance the need to safeguard national security and purposes of the DPA.

ix. The form and scope of the certificate.

x. The checks, procedures and reporting obligations placed on the Security Service as conditions of their use of the certificate.

xi. Other points on the Security Service's need for use of exemptions under the Data Protection Act 1998.

These factors are explained below.

1.3. While this document gives as full as possible account of the reasons why the Home Secretary signed the certificate, it must be remembered that there are other considerations not set out here. These considerations arise from the Home Secretary's personal detailed knowledge of the secret work of the Security Service. Obviously, these considerations cannot be made public.

1.4. This document focuses on the use of the national security exemption from the entitlement of an individual, under section 7 of the DPA, to be told by a data controller whether or not that data controller holds personal data on that individual and, if held, provide information on the data being held. Almost inevitably, a subject access request will be the first step for anyone concerned by the possibility of the Security Service processing personal data on them. The Security Service is seen to be a data controller.

2. The Data Protection Act 1998, its national security exemptions, and role of the Tribunal

2.1.The Data Protection Act 1998 (DPA) came into force on 1 March 2000. The DPA made new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

2.2. Section 7 of the DPA, created a general entitlement for an individual to ask and be told by anyone who decides on purposes of processing personal data whether personal data on them is being processed, which includes being held, and if it is, be told certain information about that data. The entitlement to ask and be told in this way is known as "subject access". The main rationale for subject access is so an individual can satisfy himself or herself as to what, if any, personal data is being processed about them, that any processing is done for a proper purpose, that the data is accurate, and to whom the data may be disclosed. If dissatisfied with the outcome of their request, the individual can then take corrective action.

2.3. The DPA recognises that there are certain circumstances when it would be inappropriate to comply with certain of the DPA's provisions, and so provides several exemptions. One, at DPA section 28, exempts personal data from a number of provisions, including those of subject access, if the exemption is required for the purpose of safeguarding national security.

2.4. DPA section 28 also provides that a Cabinet Minister may sign a certificate as conclusive evidence of the need for the use of the national security exemption. The certificate may identify the personal data to which it applies by means of a general description and may cover personal data processed after the date the certificate came into effect. Such a certificate will channel appeals against that certificate or its coverage to the National Security Panel of the Information Tribunal (the Tribunal) for consideration and determination.

2.5. The Tribunal considers appeals against a section 28 certificate by applying the principles used by the court on a judicial review. If the Tribunal determines the Minister did not have reasonable grounds for issuing the certificate or the actions in issuing the certificate were not proportionate for the purpose, the Tribunal may quash the certificate.

3. The functions of the Security Service and its primary role in the protection of national security.

3.1. The functions of the Security Service are set down in law – the Security Service Acts 1989 and 1996. It has three functions: protect national security, safeguard the economic well-being of the United Kingdom against threats posed outside of the British Islands, and - following the 1996 Act – support law enforcement agencies in the prevention and detection of serious crime. The 1996 Act defines such crime. The 1989 Act places the Security Service under the authority of the Secretary of State.

3.2. A booklet – *MI5, The Security Service* – explains in some detail the work of the Security Service. As the Service's Director General summarised in his introduction to the booklet, the Security Service's tasks are both to investigate and to counter covertly organised threats to the UK such as terrorism and espionage. The booklet explains that the Government decided that the Service should use its know-how, gained from their national security work, in support of law enforcement agencies in combating serious crime. This led to the 1996 Act. The booklet is available from the HMSO. Similar information is also available on the Security Service's Internet web site. The address is:

http://www.securityservice.gov.uk.

3.3. The work of the Security Service is vital in safeguarding the national security of the United Kingdom. Intelligence successes relating to national security can, and have:

- Saved the lives of British nationals and other persons;
- Prevented the spread of weapons of mass destruction;
- Thwarted those who would overthrow or undermine the United Kingdom's parliamentary democracy through terrorism and other means; and
- Countered the actions of foreign powers intent in damaging the interests of the country.

3.4. Members of the Security Service have no powers to question or arrest anyone, or demand entry into premises or demand to search anyone or anything. They are not like police or customs officers.

4. Why secrecy is essential to the work of the Security Service and damage and potential damage that can be done to national security when secrecy is compromised.

4.1. Secrecy is essential to the work of the Security Service. Many individuals who co-operate with the Service –such as agents - only do so under guarantee of complete confidentiality and anonymity. If their identity became known not only would it jeopardise the work in hand and their future co-operation but also it would put them at personal risk. Such a risk is not fanciful, as a large part of the Security Service's work comprises the investigation of terrorists. Clearly, the same risks apply to members of the Security Service itself.

4.2. Secrecy is also essential because the Security Service undertakes investigations covertly. The Service's effectiveness lies in its ability to obtain and exploit secret intelligence, which those under investigation may go to some lengths to keep hidden. As well as the use of agents mentioned above, sources of secret intelligence include:

a. the interception of communications,

b. eavesdropping, and

c. surveillance.

Clearly, such techniques lose much if not all of their effectiveness if it is known when and how they are used.

4.3. So, if an individual were to become aware that they were subject to a Security Service investigation, they could not only take steps to thwart it but also attempt to discover, and perhaps reveal, the methods of investigation used, or the identities of the Security Service officers, or agents involved in such methods of investigation. Compromise of methods or personnel affects both the individual investigation and potentially all other such investigations as the risk of deploying such methods and personnel is increased. Similarly, increased knowledge of methods of investigation deployed by the Security Service, and other agencies, would greatly assist those such as terrorists, spies, and serious criminals in planning their activities, so as to the reduce the likelihood of detection or interference.

4.4. Ultimately, the undermining of the effectiveness of the Security Service could result in the loss of, or a reduction in, the deterrence of those who may be tempted to damage national security. In addition, it could also result in the loss of, or a reduction in, the reputation of the Security Service itself. This could lead to a reduction in the co-operation that the Security Service actively receives from individuals and organisations both at home and abroad and also to an impairment of the ability of the Security Service itself to recruit staff. Anything that weakens the effectiveness of the Security Service weakens the UK's ability to safeguard national security.

5. The need for and use of the "neither confirm nor deny" policy.

5.1. It has been the policy of successive governments neither to confirm nor to deny suggestions put to them on the work of the intelligence and security agencies including the Security Service. Put simply, the policy is a way to preserve the secrecy described above by giving a vague and non-committal answer.

5.2. The need for such a policy and Parliament's acceptance of this is reflected in legislation. Such legislation includes the Security Service Act 1989, which places a duty on the Director General to ensure that no information is disclosed by the Service except so far as necessary for the proper discharge of its functions. It also includes the Official Secrets Acts 1911 to 1989. The 1989 Act makes it unlawful for a member of the Security Service to make any unauthorised disclosure of information held by virtue of their work, or make any such disclosure purporting to be on such information or one intended to be take as such. It also includes the predecessor to the current Data Protection Act, namely the Data Protection Act 1984. The Code of Practice on Access to Government Information, Second Edition 1997, gives "information whose disclosure would harm national security" as a category of information that is exempt from the provisions of the Code.

5.3. The Government applies the policy to Security Service investigations and to suggestions of whether a particular individual or group is or has been under investigation. To ask whether the Security Service holds personal data on an individual often amounts to asking whether there is or has been an investigation.

5.4. By logical extension, the policy must apply even if no investigation has taken place. If the Security Service said when it did not hold information on a particular person, inevitably over time those on whom it did hold information would be able incrementally to deduce that fact. Not least because they would not receive the same assurance given to others.

5.5. If individuals intent on damaging national security could confirm that they were not subjects of interest to the Security Service, then they could undertake their activities with increased confidence and vigour. Another complexity would be the handling of cases where the Service had confirmed no interest in an individual or group but subsequently it took an interest. Would the Security Service be obliged to tell the earlier enquirer that the circumstances had changed? In any event, the response to repeat requests would reveal the change in circumstances. In either case, damage is done not only in the way described in section 4, but also the timing of the change would be helpful to those under investigation. For example, a terrorist may work out what he or she had done at that time to give themselves away. If so, they, and others they told, could avoid such actions in the future - ultimately, this would help them in carrying out their acts of terror.

5.6. Conversely, confirmation to individuals that they are subjects of interest may create or fuel suspicions that associates of theirs are assisting the Security Service. The consequences of this could be harm to those who are in fact providing assistance, harm to those wrongly suspected of such assistance; and eventually in either case harm to the work of the Security Service in that the potential of personal harm to such persons would act as a strong deterrent to anyone assisting the Security Service, both in the investigation in question and in any other.

5.7. There are circumstances when the neither confirm nor deny policy is **not** used. Usually when it has been officially confirmed that the Security Service had undertaken an investigation, for example when a terrorist had been prosecuted, or when the interests of national security require a disclosure.

6. The safeguards and statutory controls that exist on the activities of the Security Service.

6.1. By their very nature, the Security Service's covert investigations are intrusive into the privacy of individuals. For this reason, there a number of constraints, oversight arrangements and safeguards placed on the Security Service. These include:

6.1.1. Legal constraints placed on the Security Service and its work, or its Director General, by Parliament through:

i. the Security Service Acts 1989 and 1996,

ii. the Intelligence Services Act 1994, and

iii. the Regulation of Investigatory Powers Act 2000. This law governs the interception of communications, the carrying out of surveillance and the use of "covert human intelligence sources", eg undercover officers or agents.

6.1.2. Oversight by the Home Secretary. This in turn includes :

i. regular meetings with the Director General;

ii. visits to Thames House to talk with staff there;

iii. advice from officials who are in daily contact with the Security Service;

iv. personal authorisation of warranted activity under the Regulation of Investigatory Powers Act 2000, and Intelligence Services Act 1994;

v. scrutiny of the Director-General's statutory Annual Report;

vi. scrutiny of the Security Service Annual Performance and Priority Report;

vii. calling for other reports where necessary;

viii. giving evidence to the Intelligence and Security Committee, considering their reports, and participating in Commons' debates on their reports;

ix. scrutiny of the reports of the independent Interception and Intelligence Services Commissioners who see everything relevant to their function.

6.1.3. Oversight by the Intelligence and Security Committee. This is an independent committee of members of both Houses of Parliament established under the Intelligence Services Act 1994. Its terms of reference are the same as most parliamentary departmental select committees. The Committee has its own Investigator who can look into and expand on the detail of evidence given to the Committee.

6.1.4. Oversight by the independent Intelligence Services Commissioner. This role was created by the Regulation of Investigatory Powers Act 2000 and combines the previous roles of the Security Service Act Commissioner and the Intelligence Services Act Commissioner. The Commissioner must hold or have held a high judicial office. As stated above, the Commissioner sees all information relevant to his or her functions.

6.1.5. Oversight by the independent Interception Commissioner. The Regulation of Investigatory Powers Act 2000 created this role although there had been a previous Commissioner under the Interception of Communications Act 1985. The Commissioner must hold or have held a high judicial office. He or she too sees all information relevant to his or her functions.

6.1.6. The Security Service's performance, plans and priorities are subject to external scrutiny by a senior Whitehall Committee known as JIC (the Joint Intelligence Committee). The resultant report is subject to approval by senior Ministers.

6.1.7. Oversight, in financial matters, by the National Audit Office.

6.1.8. Significantly in the context of data protection, the Security Service Act 1989 places duties on the Security Service's Director General concerning the obtaining and disclosure of information. The Director General must "ensure that arrangements are in place for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions

or disclosed by it except so far as necessary for that purpose or for the purpose of preventing or detecting serious crime".

6.1.9. The Regulation of Investigatory Powers Act 2000 also set up the Investigatory Powers Tribunal. This is described below.

7. Non-Data-Protection-Act Remedies

7.1. Anyone who feels aggrieved by anything which he or she believes the Security Service has done in relation to them or their property may complain to the independent Investigatory Powers Tribunal. The Tribunal will also hear claims relating to the Security Service under the Human Rights Act. Created under the Regulation of Investigatory Powers Act 2000, the Tribunal replaces the earlier Security Service Tribunal. Members of the Tribunal must qualify as lawyers. A duty to co-operate with the Tribunal is placed on everyone holding office under the Crown – this includes all members of the Security Service. There is no bar to what Tribunal members can see when looking into a complaint. If the Tribunal upholds the complaint, it can award compensation or make any other order that it sees fit. The address of the Tribunal is: PO Box 33220, LONDON SW1H 9ZQ.

8. The test that should be used to balance the need to safeguard national security and purposes of the Data Protection Act 1998.

8.1. The DPA section 28 states "personal data are exempt … if the exemption … is required for the purpose for safeguarding national security". However, the term national security is not defined. Both domestic and European courts have accepted that the Government has significant discretion in what constitutes national security. In addition, when considering safeguarding national security the courts have accepted [1] that it is proper to take a precautionary approach. That is, it is not necessary only to consider circumstances where actual harm has or will occur to national security, but also to consider preventing harm occurring and avoiding the risk of harm occurring.

8.2. Even so, the Home Secretary has balanced the need to safeguard national security against the purposes and entitlements conferred by the DPA. The risk to national security through the compromise of the work of the Security Service has been covered above. This was balanced against the factors below:

i. the consequences of an individual not knowing whether the Security Service processes personal data on them arising from a covert investigation;

ii. if processed, an individual not knowing the purpose why it is processed;

iii. if processed, an individual not knowing whether the data is accurate;

iv. if processed, to whom the data may be disclosed;

v. the consequences of, for practical purposes, denying an individual of the opportunity to challenge the purpose for processing, the accuracy of data and opportunity to challenge to whom the data may be disclosed;

[1] The House of Lord's Judgement of 11 October in the appeal of Shafiq Ur Rehman against deportation, Secretary of State for the Home Department (11 October 2001 [2001] UKHL47).

vi. the consequences to national security of the individual not correcting inaccurate personal data on him or her; and

vii. the consequences of the Information Commissioner or the courts not having a role in examining the use of the national security exemption in regard to DPA provisions.

8.3. In weighing the above factors, the Home Secretary took account of legal constraints and controls placed on the Security Service, the lack of Security Service executive powers and that their investigations in all but rare cases are kept secret.

9. The form and scope of the certificate.

9.1. The certificate has taken account of the determination of the National Security Panel of the Information in the appeal by Norman Baker MP against the previous certificate signed on behalf of the Security Service.

9.2. As expressly permitted by the DPA, the certificate identifies personal data by general description and it covers personal data processed after the date the certificate came into effect. A general description certificate reflects the primary function of the Security Service, set out in law, to protect national security. Otherwise, an individual certificate would be required for every appeal against the Security Service's use of the national security exemption. It should be noted that in the vast majority of cases the Service will need to use the exemption to preserve the neither confirm nor deny policy or to limit the extent of disclosure. The administrative burden of ad hoc certificates, taken together with the fact that only Cabinet Ministers may sign such certificates, were also factors taken into consideration for the form and scope of the certificate.

9.3. The terms of the certificate were drafted to reflect the functions of the Security Service and the terms of the Data Protection Act 1998. A proportionate approach was adopted; careful consideration was given to the range of exemptions truly required in respect of each of the different categories of personal data, so that only the necessary exemptions were certified in respect of each category.

9.4. In particular, in line with the comments of the Tribunal, the neither confirm nor deny principle is preserved, subject to some exceptions. For example, it is not to possible to sustain the principle in respect to former employees of the Security Service. Even so, it may still be necessary, to safeguard national security, to withhold information about personal data that may have been processed.

9.5. The Home Secretary was aware that the personal data covered by the certificate might have been, or might be being, processed by the Security Service in the exercise of its function to support law enforcement agencies in the prevention and detection of serious crime. However, again in line with the policy of successive governments, the Home Secretary took the view that the complete separation of the national security and serious crime functions of the Security Service was impossible. The work of the Security Service in respect of any individual may often be carried out simultaneously under both of these functions.

9.6. The methodology, operating techniques, and resources of the Security Service are common to all three of its functions. It would be impossible to maintain a "neither confirm nor deny" approach to personal data processed under the Security Service's national security function if that approach were not adopted to personal data obtained under the serious crime function. Carefully directed or persistent enquiries made by an individual in respect of the

serious crime function of the Security Service would lead to a grave risk of revealing whether the Security Service processed data in respect of that individual under its national security function. Therefore, the Home Secretary considered that exemption of all such personal data was required for the purpose of safeguarding national security. The same reasoning of course applies to the Security Service's other function of safeguarding the economic well-being of the country.

9.7. The certificate gives notice of the checks, procedures and reporting obligations placed on the Security Service as condition of their use of the certificate. These obligations are linked for the first time to the certificate in light of the Tribunal's determination mentioned in paragraph 9.1 above. The obligations ensure that while its terms are widely drawn that the Security Service will only use the national security exemption when necessary.

10. The checks, procedures and reporting obligations placed on the Security Service as condition of their use of the certificate.

10.1. The checks, procedures and reporting obligations on the Security Service are set out in the certificate, document reference **DPA/S28/TSS/2.** The Home Secretary also considered the Security Service arrangements for dealing with DPA subject access requests as set out in their internal protocol document**.**

10.2. In summary, the obligations require the Security Service to examine each subject access application and, for the purposes of safeguarding national security,:

i. decide the whether the use of the neither confirm nor deny approach is necessary,

ii. otherwise decide to what extent the national security exemption is still necessary; and

iii. to report back to the Home Secretary on the working of these arrangements.

11. Other points on the Security Service's need for use of exemptions under the Data Protection Act 1998.

11.1. When signing the certificate, the Home Secretary noted that other DPA exemptions might well also apply to the personal data covered by the certificate.

11.2. In addition, the signing of this certificate did not exclude the possible necessity of signing other national security certificates relating to personal data processed by the Security Service.

12. Conclusion

12.1. Having considered the factors above and given his knowledge of the secret work of the Security Service, the Home Secretary decided it was right for him to sign the certificate as requested by the Security Service.