



# Interception of Communications Act 1985

## Chapter 56

REPORT OF THE COMMISSIONER FOR 1999

Commissioner:

THE RT HON THE LORD NOLAN

Presented to Parliament by the Prime Minister  
by Command of Her Majesty July 2000

Laid before the Scottish Parliament  
by the Scottish Ministers July 2000

published by The Stationery Office

---

# Contents

*Subject*

Letter to the Prime Minister

Introduction

Functions of the Commissioner

Discharge of my Functions

The Extent of Interception

Section 5: Modifications

Consultation with the Commissioner

Section 6: Safeguards

Foreign and Commonwealth Office and Northern

Ireland Office Warrants

The Scotland Act 1998

The Tribunal

Errors

General

Statistical Annex

---

---

*From: The Right Honourable The Lord Nolan*

HOUSE OF LORDS  
LONDON SW1A 0PW

30 March 2000

Dear Prime Minister,

I enclose my sixth Annual Report on the discharge of my functions under the Interception of Communications Act 1985. It is of course for you to decide, after consultation with me, how much of the report should be excluded from publication on the grounds that it is prejudicial to national security, to the prevention or detection of serious crime or to the economic well-being of the United Kingdom (section 8(8) of the Act). I have again taken the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published. I hope that this is a convenient course.

*Lord Nolan*

The Rt. Hon. Tony Blair MP

10 Downing Street

London SW1A 2AA

---

---

# Annual Report of the Interception of Communications Commissioner for 1999

## Introduction

1. On 11 April 1997 I was re-appointed Commissioner under section 8 of the Interception of Communications Act 1985 (the Act) for a second three year term.
2. My present appointment as Commissioner thus expires on 10 April 2000. This will therefore be my sixth and final annual report. I will, of course, offer any such assistance as my successor may require in completing next year's Report.
3. I have followed the same practice as in previous years, of giving as much information as I can in the first part of my report. Those matters which cannot be fully explained without disclosing sensitive information relating to particular agencies or to individuals or the organisations concerned are contained in the confidential annex.

## Functions of the Commissioner

4. As Commissioner I have two main functions. The first is to keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 2 to 5 of the Act and the adequacy of any arrangements made for the purpose of section 6. The second is to give the Tribunal set up under section 7 of the Act all such assistance as the Tribunal may require for the purpose of enabling them to carry out their functions under that section. I give further information about the Tribunal in paragraphs 31 to 33 below.

## Discharge of my functions

### *Review of the Secretary of State's powers to issue warrants*

5. Whilst I have referred to the interception process in previous Reports, I believe it is important that I continue to do so for purposes of clarification and to assist understanding. Looking at the nature of interception itself, it is helpful to refer to the definition which was included in section 1.1 of the Home Office consultation paper "Interception of Communications in the United Kingdom (CM4368)" published in June 1999:

"Interception of communications occurs where a private communication between two or more parties, sent via a communications handling system, is covertly monitored in order to understand the content".

6. Within the scope of this definition there are two kinds of warrants, one for the opening of mail and the other for the interception of all forms of telecommunications including telephone, facsimile, telex and other data transmissions whereby information is communicated via a public telecommunications system. It is worth noting that "monitoring" in this context does not lead to problems with the making of telephone calls. There are technical factors, as well as the possibility of unlawful interception, which may be the cause of such problems. Likewise, official interception would not involve the abstraction of post, nor its non-delivery of post by the Post Office. Any such occurrence is likely to involve simple error or possible criminality which should be reported through established complaints channels.

7. Until recently interception warrants under section 2 of the Act have been issued only by the Home Secretary, the Foreign Secretary and the Secretaries of State for Scotland and Northern Ireland. The position has changed this year with the implementation of the Scotland Act 1998 which provides for Scottish Ministers to issue warrants for the prevention or detection of serious crime, responsibility for which in Scotland is devolved to the Scottish Executive. I give further information regarding this change in paragraphs 28-30 below.

8. Under section 2(2) the Secretary of State concerned has to satisfy himself on the facts of each case that it is necessary to issue a warrant in the interests of national security, or for the prevention or detection of serious crime, or for the purpose of

safeguarding the economic well-being of the United Kingdom. These warrants are in practice obtained on application by the National Criminal Intelligence Service, Metropolitan Police Special Branch, HM Customs and Excise, Royal Ulster Constabulary, Scottish Police, the Security Service, Secret Intelligence Service and Government Communications Headquarters, and no other agencies.

9. It is for the applicant agency to satisfy the appropriate Secretary of State that the information required is for one of the purposes set out above, and that it could not reasonably be obtained by other means. The grounds for the application are stated in writing. Each warrant sets out the name and address or telephone number of the person whose communications are to be intercepted. The warrant must be issued under the hand of the Secretary of State, save that in an urgent case he may authorise its issue by a senior official of his department. In such a case the warrant automatically lapses at the end of the second working day following the day of its issue, unless it is renewed under the hand of the Secretary of State.

10. I have continued my practice of making twice yearly "warrantry" visits to each of the departments and agencies concerned. In each case I have obtained a complete list of the warrants issued, renewed, modified or cancelled since my last visit. From these lists I have selected a sample of warrants for close inspection in order to satisfy myself firstly that the procedures adopted by each of the agencies and departments when applying for warrants are effective and provide the Secretary of State with accurate information, and secondly that the case justified the issue or the renewal of the warrant.

11. During my reviews I have had access to all the relevant files and appropriate documentation and have discussed the cases directly with the operational officers concerned to ensure that the facts warranted the use of interception, and that the officials concerned fully understand the arrangements in place to ensure that the intercept material is properly safeguarded in accordance with section 6 of the Act.

12. I have found no case in which the information supplied to the Secretary of State has been materially incomplete or inaccurate whether on the issue, renewal or modification of a warrant. Nor have I found a case where the Secretary of State has issued or renewed a warrant without adequate justification. As this is my final Report it is right for me to say that all of the Secretaries of States with whom I have had dealings in both this and previous administrations have taken great care to satisfy themselves that the warrants are necessary for the authorised purposes. I would mention in particular the Home Secretary and his predecessor, who have borne the heaviest burden and have both discharged it with exemplary thoroughness.

13. I referred in some detail in my last Annual Report to interception for the purpose of "safeguarding the economic well-being of the United Kingdom". The word "safeguarding" pre-supposes the existence of some form of threat to the economic well-being. In last year's Report I outlined discussions I had conducted with the Intelligence Services Commissioner, and the drafting of advice by lawyers in the Secret Intelligence Service, Government Communications Headquarters and the Home and Foreign Offices to clarify the distinction between the rather narrower test for interception on the grounds of economic well-being and the wider remit of the functions given to those particular agencies in sections 1(2) and 3(2) of the Intelligence Services Act. On the basis of my warrantry reviews, I can report again that the distinction between the two Acts has continued to be faithfully applied, and that warrants for interception from these agencies have remained within the narrower limits of the 1985 Act.

## The Extent of Interception

14. As in the past, the Annex to this Report contains a summary of the numbers of warrants in force at the end of 1999 and those issued throughout the course of the year by the Home Secretary and a composite figure comprising the Secretary of State for Scotland and, for the first time following implementation of the Scotland Act 1998, the Scottish First Minister. It will be seen that the number of warrants issued by the Home Secretary was one less than in 1998, but there have been 565 modification additions pursuant to the policy outlined in paragraphs 16-19 below. The great majority of warrants issued in England and Wales and Scotland remain related to the prevention and detection of serious crime. The continuing incidence of serious and organised crime and an increased facility to counter it are the main cause of the larger numbers of warrants and modifications issued. The substantial annual increases which have occurred clearly call for the exercise of vigilant supervision, but so far I have not found them a cause for concern. I have taken particular care to assure myself that the Secretaries of State are able to apply the degree of attention this increased workload imposed on them. I can report that the level of scrutiny has been and continues to be maintained, and that standards have not slipped.

## Section 5: Modifications

15. In my reports for 1997 and 1998 I referred to a proposed change of policy whereby the use of the section 5 power to modify warrants was to be extended to serious crime cases. I should explain that section 5 provides three methods of

modifying existing warrants by adding or deleting addresses (including telephone numbers). The Secretary of State may himself do so at any time. Alternatively, in an urgent case, a person holding office under the Crown may modify a warrant on behalf of the Secretary of State provided that the warrant bears a statement expressly authorising him to do so. Finally, again in circumstances of urgency, a senior official may modify a warrant on the express authority of the Secretary of State. It is only where the Secretary of State modifies a warrant that the modification exists for the full term of the warrant. Where the warrant is modified by a Crown Servant acting in the Secretary of State's stead, the modification ceases to have effect at the end of the fifth working day unless it is confirmed by the Secretary of State.

16. I explained in my report for 1997 that Government policy in relation to the modification of warrants had depended on the purpose of the warrant. Where a warrant is issued in the interests of national security, or for the purpose of safeguarding the economic well-being of the United Kingdom, the practice has been for each warrant to bear every address relating to the particular target and public telecommunications operator (PTO). Only warrants of these types had ever carried the wording which would allow senior officials to authorise emergency modifications. In serious crime cases, established policy had been one address per warrant. The Secretary of State retained the power to modify but in practice, following the one address per warrant route, had normally issued a new warrant rather than a modification instrument on a change of address. There was no legal reason or requirement for this distinction in serious crime cases.

17. Last year I reported that a new policy whereby use of the section 5 modification in serious crime warrants had been implemented in England and Wales (though not Scotland) in July 1998 in accordance with guidelines submitted for my approval. I undertook to report to you again on the effect of the change in the light of a full year's experience. I can now report that in 1999, as mentioned in paragraph 14 above, this new policy resulted in the modification of 565 serious crime warrants, the majority relating to the addition of telephone addresses. I have reviewed this practice in the course of my warrantry visits to the Departments and agencies and can report that overall the new practice has worked well. The speed of processing modifications as opposed to fresh warrant applications has increased. This fact, together with the facility for urgent modifications to be signed by officials outside office hours has operationally benefited the agencies as well as partly relieving the burden on the Secretary of State.

18. I should explain that the use of the modification procedure has not significantly increased the extent of interception. Modifications may be used only to add or delete telephone numbers from existing warrants; there is no question of increasing the number of individuals or organisations who are subject to interception. It follows, incidentally, that the bald figure for the number of warrants issued does not accurately reflect the burden imposed on the Secretary of State. A new warrant may well mean simply that a criminal or terrorist with whose file the Secretary of State is already familiar has changed his telephone number.

19. The Home Office consultation paper "Interception of Communications in the United Kingdom" (CM4368) to which I referred earlier in this report includes a proposal to replace the existing system whereby warrants specify a telephone number or address with a system of warrants which relate to the person specified upon them. This proposal is being carried forward in the Regulation of Investigatory Powers Bill. I support it. The world has changed considerably since the 1985 Act was introduced. Advances in technology coupled with developments in the telecommunications field generally have combined to an extent that the existing system, although impressive in a number of ways, can be subject to duplications of effort and unhelpful bureaucracy. In my view the proposed approach based on warrants specifying individuals would achieve a welcome overhaul and modernisation of the system whilst assisting in providing a truer and more accessible representation of the extent of interception than is currently possible.

20. There have been initial administrative problems with the application of the modification procedure which appear from the errors section of this report. A determined effort has been made to overcome these problems and they now appear to have been solved. I can also report that use of the modification procedure has been restricted to the most serious of crimes. I should be worried to see any lowering of the threshold, but it has been maintained. Professional criminals respect no boundaries and operate in a flexible and often ingenious manner. The increased use of the modification power in serious crime cases has helped to ensure that the law enforcement agencies can compete on more level terms.

## Consultation with the Commissioner

### *Application of the Urgency Procedure for issuing Interception Warrants*

21. In his Annual Report for 1998 the Intelligence Services Commissioner, Lord Justice Stuart-Smith, referred to an apparent problem with the application of the emergency procedures included in the Intelligence Services Act 1994 (ISA). An operation

had been identified where a Secretary of State had authorised the issue of a warrant in accordance with the urgency procedure in section 6(1)(b) of the ISA to an official of another Department. Lord Justice Stuart-Smith queried this practice, which appeared to fall outside the relevant section which provides that a warrant may be issued:

*"in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed thereon, under the hand of a senior official of his Department".*

Lord Justice Stuart-Smith reported that a review of the application of section 6(1)(b) was underway.

22. I have been closely involved in this review process as section 4(1)(b) of the Act includes a similar provision whereby a warrant shall not be issued except :

*"in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed thereon, under the hand of an official of his department of or above the rank of Assistant Under Secretary of State".*

Warrants issued in this way are valid for a period ending with the second working day from the date of issue. The review confirmed that there had indeed been past occasions where a Secretary of State had authorised an official of a Department other than his own to issue a warrant. Whilst there are arguments to the contrary, I am in agreement with Lord Justice Stuart-Smith that a strict application of the provisions of the Acts renders warrants issued in this way technically flawed. It is to be noted that the application of the urgency procedure has been limited to exceptional circumstances and all warrants issued under this provision have been agreed personally by a Secretary of State. But it is important that the flawed practice should be eradicated to avoid any future doubt regarding the lawfulness of warrants. I am pleased to report that changes in procedure have now been adopted in the light of the review, and there should be no future problems or scope for confusion on the application of a worthwhile and necessary provision.

### *Interception of Pagers*

23. In my last report I commented on the need for a new warrant regime to cover the interception by the police of radio pagers used by those engaged in serious crime. For the record, it will be recalled that until 1992 such activity had been considered to fall within the provisions of the Act but had been stopped following legal advice that pager systems are not subject to the Act. Since this advice was given HM Customs has relied upon section 5 of the Wireless Telegraphy Act to effect pager interception whilst the police sought production orders in the Crown Court under section 9 of the Police and Criminal Evidence Act 1984. In January 1998 a Judge sitting at Worcester Crown Court refused such an application for a production order. This decision was based on the fact that police officers are not "servants of the Crown" for the purposes of section 5 of the Wireless Telegraphy Act 1949 which makes it an offence for any person to interfere with wireless transmissions other than under the authority of a Secretary of State or someone acting on his behalf, or in the course of a person's duty as a "servant of the Crown". The Association of Chief Police Officers (ACPO) accepted this judgement insofar as it impacted on police powers and all pager intercept operations were suspended until a suitable mechanism for their authorisation had been established.

24. The Home Office and other interested parties considered this issue and concluded that a new warrant regime should be established for pager interception. The procedures adopted are based closely on the provisions of the 1985 Act, save that it is not necessary for the Secretary of State to issue such warrants personally: officials acting under his authority may perform this function. The authorisation criteria are based on the definition of "serious crime" contained in section 10(3) of the 1985 Act supplemented by certain offences relating to the supply of drugs. This system has been implemented in England and Wales since August 1998. As of 31 December 1999 a total of 77 authorisations had been given.

25. In paragraphs 26 and 27 of last year's report I reported that the Home Office had sought my agreement to oversee the issue of Wireless Telegraphy Act warrants for pager messages in much the same way as for interception warrants. On the clear understanding that pager interception would be brought within the Interception of Communications Act (or other legislation) as soon as possible, I agreed to supervise them in an unofficial capacity. Consequently, I have received lists of all pager interceptions authorised under the new procedure, and I have studied a number of individual applications based on a selection made from these lists. I can confirm that, as is the case with serious crime interception warrants, the appropriate thresholds have continued to be met and the system administered and applied with care and effectiveness, both by the applicant bodies and by the authorising Departments. I note that statutory provision for pager interception is included in the Regulation of Investigatory Powers Bill.

## Section 6: Safeguards

26. I have continued my practice of considering and discussing the arrangements made by the Secretary of State under section 6 of the Act for the purpose of limiting the dissemination and retention of intercepted material to what is necessary for the purposes of section 2 of the Act. I have been impressed by the care with which these documents are reviewed and updated in the light of technical and administrative developments. Those involved in the interception process are aware of the invasive nature of this technique, and care is taken to ensure that intrusions of privacy are kept to the minimum. There is another incentive to agencies to ensure that these documents remain effective in that the value of interception would be greatly diminished as a covert intelligence tool should its existence and methodology become too widely known. The section 6 requirements remain as important as ever. I am satisfied that the agencies continue to operate within their existing safeguards.

## Foreign and Commonwealth Office and Northern Ireland Office Warrants

27. In paragraphs 10-12 of my report for 1995 I set out the reasons for not disclosing the number of warrants issued by the Foreign Secretary and the Secretary of State for Northern Ireland in the main part of my report. I remain of the view that the disclosure of this information would be prejudicial to the public interest, but I have included them in the confidential Annex.

## The Scotland Act 1998

28. The Scotland Act 1998 was implemented on 1 July 1999. It makes the interception of communications a "reserved" subject which means that only the UK Parliament can amend the Act. National security and economic well-being are likewise "reserved" matters, remaining the responsibility of the UK Parliament. In general, however, responsibility for policing and criminal law is now devolved to the Scottish Parliament and is ultimately the responsibility of Scottish Ministers. In recognition of this fact, it was agreed that as of 1 July 1999 responsibility for authorising serious crime warrants in Scotland should be transferred to Scottish Ministers. In practice, this function is exercised by the First Minister of the Scottish Executive and his Deputy (another member of the Executive). This result has been achieved by an executive devolution of the Secretary of State's functions under section 63 of the Scotland Act 1998 whereby Scottish Ministers are permitted to exercise functions "in or as regards Scotland".

29. The new arrangements for Scotland build upon the exemplary efficiency of the previous system. They provide that Scottish Ministers have sole competence to issue a warrant on serious crime grounds where:

- a) the person specified on the warrant is known to be in Scotland when the warrant is issued;
- b) the person specified on the warrant is reasonably believed by the Scottish Ministers to be located in Scotland at the time when the warrant is issued; or
- c) the persons specified on the warrant are located in Scotland.

I have visited the Scottish Executive and have reviewed the procedures in place. I am satisfied that applications are closely scrutinised at a number of levels, both within the agencies and within the Executive, before being presented to Scottish Ministers. Procedures have also been devised and implemented to ensure that the high level of service and assistance provided to the Tribunal is maintained.

30. The only concern I would record arises out of the arrangements put in place for national security and economic well-being warrants relating to Scotland. Before devolution they, like Scottish serious crime warrants, were the responsibility of the Secretary of State for Scotland. Now they are the responsibility of the Home Secretary. This arrangement reflects the established primacy of the Security Service in cases involving terrorism. I understand that procedures are in place on the ground to avoid potential difficulties or failures of communication in the warranting, administrative and operational processes. That said, I believe that the working of this aspect of the system will need to be kept under review as the post devolution system establishes itself further.

## The Tribunal

31. The Tribunal, which comprises five senior members of the legal profession, is independent of Government. The President is Sir William Macpherson of Cluny. Upon an application being made to the Tribunal it will investigate whether the Secretary of State has authorised the interception of a person's mail or telephone calls entrusted to the Post Office or to Public Telecommunications Operators. Unless the Tribunal considers a complaint to be frivolous or vexatious it must investigate to ascertain whether the Secretary of State has issued an interception warrant. If such a warrant does exist the Tribunal must determine whether the Secretary of State had reasonable grounds for issuing the warrant.



32. The Tribunal received 69 new applications during 1999 and completed the investigation of 67 of these during the year as well as concluding its investigation of the 3 outstanding cases from 1998. 2 other cases have been carried over from 1999. On no occasion has the Tribunal concluded that there had been a contravention of sections 2-5 of the Act.

33. The Tribunal requested my assistance in 1999 in one case in accordance with my function provided by section 8(1)(b) of the Act. It is not possible to discuss this request without revealing information of a sensitive nature, and I have therefore described it in the confidential annex.

## Errors

### *Public Telecommunications Operators (PTOs)*

34. In the first case, the PTO commenced an interception for the Security Service. The Service expected to receive another line and queried the number provided. The PTO insisted the correct number was being provided. The Service quickly established that they had indeed received the wrong number. The intercept was immediately suspended. An investigation of the problem established that both HM Customs and the Security Service were awaiting intercepts and the numbers had been programmed incorrectly by the PTO. All product received has been destroyed and the PTO's procedures tightened to avoid a recurrence.

35. In a second case involving a quick moving operation a PTO provided the Security Service with an intercept against an incorrect number. This problem resulted from human error and the PTO has reviewed procedures to minimise the potential for a recurrence.

36. In a third case, the Security Service continued to receive product from a PTO following the change of a subscriber's telephone number. The new number had not been the subject of a warrant but had nonetheless been intercepted because of the technical nature of the interception process involved. All product from the unauthorised interception was immediately destroyed. The technical nature of this error, which I cannot detail without reference to sensitive material, poses problems for the warrant process. It is rather harsh to attribute blame to the PTO. The error resulted from a very unusual set of circumstances. I understand that the potential for future occurrence of this problem is slight but close scrutiny of this problem should be maintained to guard against repetition.

37. A further error occurred when the Security Service was passed product from a National Criminal Intelligence Service warrant on an unrelated target. The error resulted from the PTO changing procedure for the allocation and supply of intercepts without informing the intercepting agencies. This error resulted in the interception of one unrelated call which has now been deleted from all systems. The PTO has organised a meeting to inform all relevant parties of the new procedure and there should be no recurrence of this problem.

38. A separate problem was caused by another PTO updating part of its interception system without pre-warning the intercepting agencies. This led to incompatibility problems and the Security Service receiving product supposedly relevant to two warrants but actually comprising four rogue calls. All systems are now compatible and there should be no further problems of this nature. I find this and the preceding error disappointing. These two errors should not have occurred and the PTOs must recognise the importance of effective communication to reduce the scope for future problems of this nature.

39. A further error occurred following the Security Service undertaking a feasibility check with a PTO. An application for a warrant was not made following this check. Feasibility was subsequently rechecked and the PTO advised that an application for a warrant would soon be made. The PTO undertook preparatory action but due to a breakdown in communication product was made available to the Security Service without notification having been received that a warrant had been signed. The error was identified by the Service and all product received in the short intervening period destroyed. The alertness of the Service in so promptly detecting the above PTO errors is highly commendable.

40. A further error occurred where a PTO employee entered an incorrect number whilst upgrading an internal system. The fact that this error occurred during an upgrade makes similar mistakes unlikely.

41. A further error occurred where incorrect information was specified by a PTO to GCHQ. This led to the signature of a modification to a warrant including incorrect information. The PTO quickly identified the problem on receipt of the modification instrument, and action was taken to correct it as soon as practicable. The PTO was quick to identify the error and no improper interception took place.

42. In another case, a warrant was issued on behalf of HM Customs. It quickly became apparent that the telephone subject to interception was at a different address and unknown persons were using it. The intercept was immediately cancelled and all

product destroyed. The PTO made enquiries and established that incorrect product had been provided to HM Customs. Steps were taken to resolve the matter but, unfortunately, the first call then intercepted included unrelated material. The intercept was again immediately ceased and the product of the one call destroyed. The PTO were again advised of the error and confirmed that the problem was due to a complicated technical problem which they were required to rectify. Whilst there will occasionally be problems of a technical nature, it was particularly unfortunate that this one was not resolved by the PTO when the first error was identified.

43. Finally, an error occurred when the product of properly authorised and warranted interceptions was routed to the wrong agencies. This error was quickly identified by the agencies and investigation confirmed that the problem had occurred when a technical system was updated. I am advised that the new system is now in place and the problem leading to this unfortunate cross-over of product resolved.

## *The Home Office*

44. A procedural mistake occurred within the Home Office when HM Customs and Excise applied for the cancellation of a warrant following the full identification of a target. The application also requested a warrant in the individual's true identity. It is standard practice in such cases for the cancellation instrument to be signed after the new warrant has been issued thereby maintaining continuity of interception. However, in this particular case the cancellation instrument was signed the day before the new warrant, which led to a period of unwarranted interception. The error was identified by the PTO following receipt of the cancellation instrument and any product obtained during the period of unwarranted interception has been destroyed.

## *The Security Service*

45. In the first case the Security Service applied for a revalidation of a warrant, but the submission listed an incorrect operator. This initial error was not identified by the Home Office and the warrant was renewed including the incorrect operator. This renewal was therefore invalid. This error only came to light when an approved request to modify the warrant to delete one number and add another was submitted to the original operator. The error was compounded by the fact, confirmed by subsequent investigation, that given the particular circumstances of this operation, the intercept had not been suspended when it should have been. This increased the period of unlawful interception. All product from the total period subject to the error has been destroyed. The error reflects badly on all parties concerned, the Security Service, the Home Office and the operators involved.

46. In a second case, due to human error at the Security Service, a wrong number was added to a warrant. The intercept was suspended as soon as the error was discovered and no product was received. The importance of effective checking has been stressed to operational personnel.

47. In a third case, the error resulted from an incorrect number being targeted by the Operator. Investigation has failed to establish the precise reason why the incorrect number came to be intercepted. It would appear that this error had been caused by human failing on the part of one or more of the parties involved in the interception process.

48. In another case a change in a target number combined with the nature of the method of interception deployed resulted in unwarranted interception. This error resulted from a failure within one part of the Service to realise that the method of interception deployed would lead to continued receipt of product following a number change, and a corresponding failure by transcribers to alert the warantry team that intercept had continued. The intercept was suspended immediately the relevant section became aware that interception had continued following the number change. All product received after the number change has been destroyed. Relevant sections have been advised of the susceptibility of this method of interception to the problem and written guidance has been circulated to transcribers so as to avoid this type of breach in the future.

## *Government Communication Headquarters*

49. In the first case, a particular warrant included an incorrectly specified number. The error was identified and no interception took place. The incorrect number was subsequently deleted from the warrant. The error could and should have been prevented if normal practice including subscriber checks had been applied. Steps have been taken to ensure that this important safeguard is built into the warantry process.

50. In another case I have been advised of a problem relating to the safeguards under section 6 of the Act. I describe this problem in the confidential annex to this report because it cannot be fully explained without referring to confidential information. I can report that this problem involved no unlawful interception and that suitable action has been taken to ensure

that the safeguards continue to be complied with.

## *National Criminal Intelligence Service*

51. In one case, NCIS requested the cancellation of a warrant. A cancellation instrument was duly issued. A further cancellation request was made some three weeks later. It then became clear that the intention of NCIS, which had been communicated to the PTO, was initially to seek a modification deletion of only one of the numbers included on the warrant, the first cancellation request having been submitted in error. The PTO should, of course, have ceased interception on receipt of the initial cancellation request. In fact, the PTO complied with the intention of NCIS (implementing only the modification deletion) with the result that a period of unauthorised interception of 13 days occurred.

52. A similar mistake was made in another case. A warrant was modified with the addition of a number. NCIS subsequently erroneously requested the cancellation of the warrant when they in fact wished to delete a number from the warrant only. A cancellation instrument was subsequently issued, and the error came to light. The PTO had continued to intercept a number included on the original warrant. Monitoring was immediately terminated but unauthorised interception occurred for one day.

53. A third error occurred where NCIS sought cancellation of a warrant against a target. This request was quickly followed by a further application for a warrant against the target. The Home Office caseworker agreed with NCIS that the cancellation and application should be treated as a modification addition and deletion to the existing warrant. When NCIS subsequently terminated one of the numbers, it became clear that the initial warrant had not been renewed. Remaining interception which had been subject to the warrant was suspended immediately, but this error resulted in a period of unauthorised interception of two lines for 18 days.

54. A further error occurred regarding a warrant to which a number had been added by a modification addition on 7 July 1999. It subsequently transpired that the warrant had not been renewed, and had expired on 2 July. Interception was terminated on 15 July resulting in a period of unauthorised interception of 13 days. This error appears to have occurred as a result of deficiencies in checking on the part of the Home Office and NCIS. NCIS has undertaken a review of their administrative procedures following discovery of this breach and have introduced a checking system which should minimise the potential for recurrence. The Home Office is also piloting a new system which will enable the identification of warrants that are live and due for renewal together with those that have been cancelled. I welcome these developments. It is important for the integrity of the warranting process that simple errors of this nature are eradicated.

55. A further error occurred when, due to a typographical error, an inaccurate number was included in an application for a warrant. The error was identified immediately and the interception terminated. A review of application procedures in the applicant office has been undertaken.

56. I should add that these errors occurred when the modification procedure for serious crime warrants remained in its infancy. They highlighted a number of problems in the administrative and checking procedures of the Home Office, the agencies and PTOs alike. Action has been taken to tackle this problem including a seminar attended by all parties and a series of visits and meetings. I am assured that this action has resulted in a more effective operation of the procedure.

57. I have also been advised of a breach of the section 6 safeguards which occurred in March 1999. An accredited police reader of intercept material correctly recorded details of a warranted interception on an authorised log sheet. This was correctly sanitised and coded in accordance with established practice. Unfortunately, the officer subsequently left the log sheet on a train. He immediately notified his senior officers and NCIS, and the British Transport Police were able to recover the log sheet. The envelope containing the log had been opened but the content was intact and there was no evidence that it had been read. An internal enquiry has been carried out by NCIS and the police force concerned. This confirmed that apart from the very serious failing of the log having been mislaid, the other requirements of the safeguards had been followed. No compromise of the operation has been apparent as a result of this incident. The officer involved has been dealt with in accordance with internal discipline.

## *NCIS Inquiry*

58. I explained in my last report that I had been informed by the Deputy Director General of NCIS that a serious breach of the section 6 safeguards had occurred in relation to some of their interception product. In the course of an operational liaison with the police of another European country, a senior investigating officer of an English Constabulary disclosed, in writing, that the targets' communications were subject to interception under warrant. I explained further that the investigating officer's report into this matter had only recently been received, and I undertook to report to you again.

59. I subsequently submitted a report to you in August 1999 in accordance with section 8(5)(b) of the Act. Whilst I do not intend to provide any factual detail in this present Report, as to do so would involve disclosing information of a sensitive nature, I believe I should refer to certain aspects of the incident so that the public may be properly informed.

60. The full Report into the matter followed an Inquiry undertaken by a Superintendent at NCIS. It concluded that there had indeed been breaches of the existing section 6 safeguards and that inappropriate disclosures had been made to the European police force concerned.

61. The unauthorised disclosures had occurred in 1996. They therefore predated the greatly improved system for the handling of interception material implemented at NCIS and throughout the police service generally following an Inquiry by John Stevens, then Chief Constable of Northumbria Police. I referred in detail to this Inquiry in my report for 1997 (paragraphs 53-56). I believe that if this improved system had been in force it would almost certainly have prevented the problems upon which I now report. But further work is needed both on the difficult question of sharing intercept material with foreign agencies and on the penalties for improper disclosure.

62. In my initial report to you in August I endorsed the adoption of what was initially an NCIS recommendation that a policy be formulated in conjunction with all relevant Departments and intercepting agencies on the disclosure of UK interception (both its existence and product) to overseas law enforcement agencies. You accepted this recommendation, and the Home Office is taking the lead responsibility in carrying this matter forward.

63. My consideration of this incident also led me to consider in general policy terms the lack of a sanction in the Act for breaches of the safeguard rules, this matter being covered presently by provisions contained in the Official Secrets Act 1989 (OSA).

64. The relevant OSA provisions include section 4(1) which makes it an offence for a Crown Servant to disclose any information, document or other article to which the section applies "without lawful authority". By virtue of section 4(3)(a) the section applies to:

"any information obtained by reason of the interception of communications in obedience to a warrant issued under section 2 of the Interception of Communications Act 1985, any information relating to the obtaining of information by reason of any such interception and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such interception".

Section 7(1) provides that a disclosure by the person concerned is made with lawful authority:

"if, and only if, it is made in accordance with his official duty".

Under section 7(4) it is a defence for a person charged to prove:

"that at the time of the alleged offence he believed that he had lawful authority to make the disclosure in question, and had no reasonable cause to suggest otherwise".

Finally, section 9(1) provides that no prosecution under section 4(1) or (3)(a) is to be instituted except by or with the consent of the Attorney-General.

65. I expressed the view based on some research I requested be undertaken that further work would be desirable to consider the ambit of section 7(1) and the scope of the section 7(4) defence in cases where a breach of the section 6 safeguards of the Act had been identified. The OSA provisions represent the only legal sanction against breach of the section 6 safeguards, and in my view, based on my consideration of this error, their effect needs to be clarified. I understand that work in this regard is also being taken forward and that appropriate provision will be included in the Regulation of Investigatory Powers Bill.

## *HM Customs and Excise*

66. An error occurred when on 25 January HM Customs requested a modification to a warrant to add a number. On 26 January HM Customs mistakenly requested the cancellation of the warrant when their intention was to seek the modification of the warrant by the deletion of one telephone number. Both HM Customs requests were considered by the Home Office at the same time, but it was not noticed that they referred to the same warrant. A cancellation request was signed on 1 February. A modification instrument to add two numbers subsequently signed on 2 February was rendered ineffective. The PTO should have ceased the interception of both numbers on the warrant. In fact, they did what HM Customs wanted and continued to intercept one of the numbers, even though the warrant was cancelled. HM Customs identified this error on 4 February. All

product recorded during this period has been destroyed. This error is similar in nature to those detailed above. HM Customs attended the workshop organised by the Home Office referred to in paragraph 56 above. This workshop has resolved many of the problems which occurred around the introduction of the modification procedure in serious crime cases.

67. In another case, it was apparent from the first call intercepted that neither party was the intended target of the intercept, which was immediately suspended. Investigation revealed that an incorrect telephone number had been inserted in the warrant application. This interception took place for less than two hours in which time only one call had been monitored. Product of this call was destroyed, and the officer involved in the preparation of the warrant application advised of the need for accuracy in this sensitive area of work.

68. A third error is similar in nature to that detailed in paragraph 67 above. HM Customs requested the cancellation of a warrant, but before this request could be actioned in the Home Office a further application was made to intercept another telephone utilised by the same target. The Home Office agreed that the extant warrant should be modified to delete one number and add the other. The modification was signed on 1 July but due to an oversight in the Home Office the warrant was not submitted for renewal and expired on 2 July. The error was identified on 22 July after a total of 20 days unwarranted interception. The oversight in the Home Office was compounded by HM Customs failing to notice that the warrant had not been included for renewal. All parties concerned, that is HM Customs, the Home Office and the PTO have taken action to avoid such oversights in the future.

## *The Post Office*

69. The Security Service received a copy of a letter sent to an address which was not subject to an interception warrant. The letter had been opened in error having been mis-sorted at the distribution office and mistaken as a letter to an address subject to a postal interception warrant. The Security Service immediately identified the error and returned the letter to the post office. Investigation revealed that this breach was due to human error. Post sorting arrangements have been changed and new checking procedures introduced to avoid any recurrence of this problem.

## *Northern Ireland Office*

70. An error was identified following the interception of six calls. A transcriber raised suspicions that the intercept was not operating against the correct target. Interception was suspended immediately. Investigation confirmed that an error has occurred following a misunderstanding regarding the target address when the warrant application was prepared. Although a number of checks were carried out prior to the intercept being activated, a final check with the relevant supervisor which should have identified the error was precluded given the urgent requirement then prevalent. The need to implement thorough checks has been emphasised to all involved, as has the requirement for applications to be shown to the senior originating officer before processing. This together with a subsequent review of procedure should prevent any recurrence.

## **General**

71. In conclusion I would like to say that throughout my term of office I have been highly impressed with the skill, determination and patience of the men and women who carry out the monitoring and transcription of telephone conversations. Their pride in the successes achieved is fully justified. My overall impression is that the statutory scheme is administered with admirable care and a strong sense of duty. In 1999, as in previous years, interception has made a very significant contribution to the well-being of the nation, and one that could not have been achieved by other means.

---

---

# Annex to the report of the Commissioner for 1999

## Warrants (a) in force on 31 December 1994 and (b) issued during the course of 1994

|                                 | <i>Telecommunications</i> |     | <i>Letters</i> |    | <i>Total</i> |     |
|---------------------------------|---------------------------|-----|----------------|----|--------------|-----|
|                                 | a                         | b   | a              | b  | a            | b   |
| Home Secretary                  | 308                       | 871 | 51             | 76 | 359          | 947 |
| Secretary of State for Scotland | 28                        | 90  | 9              | 10 | 37           | 100 |

## Warrants (a) in force on 31 December 1995 and (b) issued during the course of 1995

|                                 | <i>Telecommunications</i> |     | <i>Letters</i> |    | <i>Total</i> |     |
|---------------------------------|---------------------------|-----|----------------|----|--------------|-----|
|                                 | a                         | b   | a              | b  | a            | b   |
| Home Secretary                  | 356                       | 910 | 49             | 87 | 405          | 997 |
| Secretary of State for Scotland | 64                        | 137 | 8              | 1  | 72           | 138 |

## Warrants (a) in force on 31 December 1996 and (b) issued during the course of 1996

|                                 | <i>Telecommunications</i> |      | <i>Letters</i> |    | <i>Total</i> |      |
|---------------------------------|---------------------------|------|----------------|----|--------------|------|
|                                 | a                         | b    | a              | b  | a            | b    |
| Home Secretary                  | 431                       | 1073 | 46             | 69 | 477          | 1142 |
| Secretary of State for Scotland | 63                        | 228  | 0              | 0  | 63           | 228  |

## Warrants (a) in force on 31 December 1997 and (b) issued during the course of 1997

### *Telecommunications Letters Total*

|                                 | a   | b    | a  | b  | a   | b    |
|---------------------------------|-----|------|----|----|-----|------|
| Home Secretary                  | 420 | 1391 | 40 | 65 | 460 | 1456 |
| Secretary of State for Scotland | 38  | 256  | 0  | 0  | 38  | 256  |

## Warrants (a) in force on 31 December 1998 and (b) issued during the course of 1998

|                                 | <i>Telecommunications</i> |      | <i>Letters</i> |     | <i>Total</i> |      |
|---------------------------------|---------------------------|------|----------------|-----|--------------|------|
|                                 | a                         | b    | a              | b   | a            | b    |
| Home Secretary                  | 385                       | 1646 | 48             | 117 | 433          | 1763 |
| Secretary of State for Scotland | 53                        | 267  | 1              | 1   | 54           | 268  |

## Warrants (a) in force on 31 December 1999 and (b) issued during the course of 1999

|                                  | <i>Telecommunications</i> |      | <i>Letters</i> |    | <i>Total</i> |      |
|----------------------------------|---------------------------|------|----------------|----|--------------|------|
|                                  | a                         | b    | a              | b  | a            | b    |
| Home Secretary                   | 484                       | 1645 | 38             | 89 | 522          | 1734 |
| Secretary of State for Scotland* | 45                        | 288  | 0              | 0  | 45           | 288  |

