



Regulation of Investigatory Powers Act 2000

Chapter 23

REPORT OF THE INTERCEPTION OF
COMMUNICATIONS COMMISSIONER
FOR 2000

Commissioner:
THE RT HON SIR SWINTON THOMAS

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

Laid before the Scottish Parliament by the
Scottish Ministers

October 2001



Regulation of Investigatory Powers Act 2000

Chapter 23

REPORT OF THE INTERCEPTION OF
COMMUNICATIONS COMMISSIONER
FOR 2000

Commissioner:
THE RT HON SIR SWINTON THOMAS

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

Laid before the Scottish Parliament by the
Scottish Ministers

October 2001

Contents

<i>Subject</i>	<i>Page</i>
Letter to the Prime Minister	4
Introduction	5
Functions of the Commissioner	5
Discharge of my functions	5
The extent of interception	8
Safeguards	8
Codes of Practice	8
Foreign and Commonwealth Office and Northern Ireland Office Warrants	8
Staffing of the Secretariat	9
The Tribunal	10
<i>The Interception of Communications Tribunal</i>	10
<i>The Investigatory Powers Tribunal</i>	10
Assistance to the Tribunal	11
Errors	11
Conclusion	14
Statistical Annex	15

From: The Right Honourable Sir Swinton Thomas

The Interception of Communications Commissioner
c/o 50 Queen Anne's Gate
London SW1H 9AT

2 August 2001

Dear Prime Minister

I enclose my first Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. 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, to the economic well-being of the United Kingdom, the continued discharge of the functions of any public authority whose activities include activities subject to my review (section 58(7) of the Act). Following the practice of my predecessor, I have 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the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published.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.

Sir Swinton Thomas

The Rt Hon Tony Blair MP
10 Downing Street
London SW1A 2AA

Annual Report of the Interception of Communications Commissioner for 2000

Introduction

1. I was appointed the Interception of Communications Commissioner on 11 April 2000 in succession to the Rt Hon Lord Nolan. He and I worked together until 31 July 2000, when I effectively retired from the Court of Appeal and was able to give the time necessary for the requirements of this post. I am grateful to Lord Nolan for his assistance and invaluable advice.

2. 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 that 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

3. I was appointed under the provisions of the Interception of Communications Act 1985 (IOCA), and as from 2 October 2000 under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). The coming into force of RIPA on that date coincided with the coming into force of the Human Rights Act 1998 (HRA) which incorporated the European Convention on Human Rights into UK law. These two important pieces of legislation brought about a number of changes in the law and practice of those responsible for the lawful interception of communications.

4. As Commissioner I have two main functions; both clearly defined by the two Acts in force during the year 2000: 1 January 2000 to 1 October 2000 (Interception of Communications Act 1985) and 2 October 2000 to 31 December 2000 (the Regulation of Investigatory Powers Act 2000). 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 IOCA (sections 7 to 11 of RIPA) and the adequacy of any arrangements made for the purpose of section 6 of IOCA (sections 15–16 of RIPA). The second is to give the Tribunal set up under section 7 of IOCA (section 65 of RIPA) 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 21 to 26 below.

Discharge of my functions

5. Article 8(1) of the European Convention on Human Rights provides that everyone has the right to respect for his private and family life, his home and his correspondence. Interception of a person's communications is clearly a breach of Article 8(1). However, Article 8(2) provides: "*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, or the protection of health or morals, or for the protection of rights and freedoms of others.*" These provisions in the Human Rights Act are mirrored, but in much greater detail, in RIPA.

6. Section 1 of RIPA provides that it shall be an offence for a person intentionally and without authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public postal service or a public telecommunications system or a private telecommunications system. Sections 2 to 11 lay down detailed provisions whereby interception of communications may be made lawful, and importantly that interception can only take place after the issue of an interception warrant and that, save in exceptional and limited circumstances, a warrant can only be issued under the hand of a Secretary of State. The function of authorising warrants in respect of serious crime in Scotland is exercised by Scottish Ministers (in practice the First Minister or, in his absence, the Deputy First Minister).

7. By section 5(2) of RIPA the Secretary of State may not issue an interception warrant unless he believes that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. By section 5(3) a warrant can only be issued if it is necessary:

- a. in the interests of national security;
- b. for the purpose of detecting or preventing serious crime;
- c. for the purpose of safeguarding the economic well-being of the United Kingdom; or
- d. for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

8. Although the coming into effect of the Human Rights Act and RIPA did not bring about any fundamental change in the approach to the interception of communications in the sense that under the previous legislation the interception of communications was a criminal offence save as provided under the Interception of Communications Act 1985, and other relevant legislation, the new legislation caused the various Agencies concerned in this work, in particular the Security Service, the Secret Intelligence Service, GCHQ, the National Criminal Intelligence Service, the Metropolitan and the Scottish police forces, HM Customs and Excise, the Foreign Office, the Home Office, the Scottish Executive and the Royal Ulster Constabulary to study the new legislation with great care and to ensure that their practices were in accordance and compatible with it. A great deal of work and effort was expended on this task by the responsible persons in each of the government departments and Agencies referred to above, and also by the Communications Service Providers (CSPs). On a number of occasions I was consulted by the relevant Agencies. They were anxious to ensure that their work and practices were lawful and compatible in the context of the new legislation and I was able to advise them that, in my judgement, they were.

9. Section 57(2) of RIPA provides that as the Interception of Communications Commissioner I shall keep under review:

- a. the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under sections 1 to 11;
- b. the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I;

- c. the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties and conferred or imposed on him by or under Part III; and
- d. the adequacy of the arrangements by virtue of which:
 - i. the duty which is imposed on the Secretary of State by section 15, and
 - ii. so far as is applicable to information obtained under Part I, the duties imposed by section 55 are sought to be discharged.

Chapter II of Part I and Part III are not yet in force.

10. In accordance with these duties I have visited the Security Service, the Secret Intelligence Service, GCHQ, the National Criminal Intelligence Service, the Special Branch of the Metropolitan Police, the Strathclyde Police, the Royal Ulster Constabulary, HM Customs and Excise, the Foreign Office, the Home Office and the Scottish Executive at least twice since my appointment. I have been very impressed by the quality and the dedication and the enthusiasm of the personnel carrying out this work on behalf of the Government and the people of the United Kingdom. They have a detailed understanding of the legislation and strive assiduously to comply with the statutory criteria and, in my view, there is very little, if any, danger that an application which is defective in substance will be placed before the Secretary of State. Where errors have occurred, which I refer to below (and in detail in the confidential annex) these have been errors of detail and not of substance. Where errors occur they are reported to me and the product immediately destroyed. The Agencies have made available to me everything that I have wished to see or hear about. They welcome the oversight of the Commissioner, both from the point of view of seeking his advice, which they do quite frequently, and as a reassurance to the general public that their activities are overseen by an independent person who has held high judicial office. I am also left in no doubt as to their anxiety to comply with the law. In a case of doubt or difficulty, they do not hesitate to consult me.

11. During my visits to the security, intelligence and law enforcement agencies I took the opportunity of discussing with them the impact that implementing RIPA has had on their work. I thought it would be helpful to highlight, in the confidential annex, some examples of the Agencies' experiences of the new legislation. As this Report only covers the first three months of RIPA it is difficult to provide an authoritative assessment of its full impact. I shall be able to do so in my next report covering the year 2001.

12. I have also seen the Home Secretary on more than one occasion since my appointment, and the Secretary of State for Northern Ireland, and the Secretary of State for Defence. I have yet to meet the Foreign Secretary and First Minister for Scotland. Again, I have been impressed with the care that they take with their warrantry work, which is very time consuming, to ensure that warrants are issued only in appropriate cases and, in particular, in ensuring that the conduct authorised is proportionate to what is sought to be achieved by the interception.

13. I have also visited the Communications Service Providers (CSPs), that is to say the Post Office and all the major telephone companies. Each of the CSPs employs personnel who are engaged solely on the execution of interception of communications warrants. They acquire expertise in their field and, again, in the course of my visits, I was impressed by the care, interest and dedication of these employees to their work in this field.

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 2000 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 the Scottish First Minister. 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. The substantial annual increases which have occurred and have resulted in a corresponding increase in the workload of the Secretaries of State and on the part of the relevant Agencies clearly call for the exercise of vigilant supervision. I can report that the level of scrutiny has been and continues to be generally well maintained. That said, I am concerned about the number of errors reported during the year. I have been assured that changes have been put in place to try and ensure that there is no repetition of these in the future. I will, of course, continue to monitor the system to satisfy myself that every effort is being made to prevent such recurrences and seeking full explanations where the systems fail.

Safeguards

15. Sections 15 and 16 of RIPA lay a duty on the Secretary of State to ensure that arrangements are in force as safeguards in relation to dissemination, disclosure, copying, storage and destruction etc. of intercepted material. Again these sections require careful and detailed safeguards to be drafted by each of the Agencies referred to earlier in this Report and for those safeguards to be approved by the Secretary of State. Again my advice and approval were sought and given in respect of the safeguard documents either before or shortly after 2 October 2000. The Home Secretary also sought my advice in relation to them and they were approved by him. Separate safeguards were also approved by the First Minister for Scotland, and the Secretary of State at the Foreign Office noted with approval GCHQ's safeguards.

Codes of Practice

16. Section 71(a) of RIPA requires the Secretary of State to issue one or more Codes of Practice relating to the exercise and performance of duties in relation to Parts I to III of the Act. The Home Secretary, having first obtained my views and interim approval of the draft Code of Conduct prepared by the Home Office, gave his approval to the draft Code on the basis that he wished to see an updated Code of Conduct at a later date when RIPA had been in force for a time and all those concerned had had sufficient time to consider fully the implications of the legislation. I understand that a further draft Code of Practice is being prepared by the Home Office in consultation with the relevant Agencies and this should be placed before the Home Secretary for approval shortly.

Foreign and Commonwealth Office and Northern Ireland Office Warrants

17. In paragraphs 10–12 of my predecessor's 1995 Report, he 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 the Report. I take this opportunity to outline the reasons behind this decision.

18. This practice is based on paragraph 121 of the Report of the Committee of Privy Councillors appointed to inquire into the interception of communications and chaired by Lord Birkett. The Birkett Committee thought that public concern about interception might to some degree be allayed by the knowledge of the actual extent to which interception had taken place. After carefully considering the consequences of disclosure upon the effectiveness of interception as a means of detection, they decided that it would be in the public interest to publish figures showing the extent of interception, but to do so only in a way which caused no damage to public interest. They went on to say:

“We are strongly of the opinion that it would be wrong for figures to be disclosed by the Secretary of State at regular or irregular intervals in the future. It would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of the interceptions of communications for security purposes.”

19. Like my predecessors I am not persuaded that there is any serious risk in the publication of the number of warrants issued by the Home Secretary and the Secretary of State/First Minister for Scotland. This information does not provide hostile agencies with any indication of the targets because as Lord Lloyd said in his first Report published in March 1987: *“The total includes not only warrants issued in the interest of national security, but also for the prevention and detection of serious crime.”* These figures are therefore set out in the annex to this Report. However, I believe that the views expressed in Lord Birkett’s report still apply to the publication of the number of warrants issued by the Foreign Secretary and the Secretary of State for Northern Ireland. I also agree with the view of my predecessor, Lord Nolan, that the disclosure of this information would be prejudicial to the public interest. I have, therefore, included them in the confidential annex.

Staffing of the Secretariat

20. Section 57(7) of RIPA provides that the Secretary of State shall, in consultation with the Commissioner, provide the Commissioner with such staff as are sufficient to secure that the Commissioner is able properly to carry out his functions. The staff serving me as Commissioner also serve the Intelligence Services Commissioner and the Tribunal. Just prior to my appointment, the Secretary to the Commissioner was promoted leaving the office vacant. It took some time to appoint a successor. Once a successor had been appointed it quickly became apparent that the workload was far too great for one person, and that an increase in staff was essential. It is not easy to identify persons who are suitable for these posts, and, once identified, they must be vetted and cleared for security purposes to a high level, and this also takes time. There is no doubt that the situation was unsatisfactory for a period of time but the staff have now been increased to three plus a part-time Registrar for the Tribunal and I trust that this will be satisfactory for the time being. However, the work of the Commissioner and his staff will increase substantially when Chapter 2 of Part I of RIPA comes into force. You will remember that the Rt Hon Mr Tom King, CH, MP, the Chairman of the Intelligence and Security Committee, having asked Sir Simon Brown and myself certain questions about staffing when we gave evidence to the Committee, wrote to you in December 2000 expressing understandable concern in relation to the Secretariat but, as I have said, I trust that the problem which he rightly drew to your attention has now been cured.

The Tribunal

21. With the introduction of the Regulation of Investigatory Powers Act 2000 on 2 October 2000 the Interception of Communications Tribunal, established by virtue of section 7 of the Interception of Communications Act 1985, ceased to exist. To give a complete picture of the complaints considered by both Tribunals the following are separate reports of their work.

The Interception of Communications Tribunal

22. The Tribunal, which comprises five senior members of the legal profession, is independent of Government. The President is Mr Justice Burton. 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.

23. The Tribunal received 60 new applications during 2000 and completed the investigation of 14 of these during the year as well as concluding its investigation of the two outstanding cases from 1999. Forty-six cases have been carried over to 2001. On no occasion has the Tribunal concluded that there had been a contravention of sections 2–5 of the Interception of Communications Act 1985.

The Investigatory Powers Tribunal

24. The Investigatory Powers Tribunal was established by section 65 of the Regulation of Investigatory Powers Act 2000. The Tribunal came into being on 2 October 2000. From that date the Investigatory Powers Tribunal assumed responsibility for the jurisdiction previously held by the Interception of Communications Tribunal, the Security Service Tribunal and the Intelligence Services Tribunal and the complaints function of the Commissioner appointed under the Police Act 1997 as well as claims under the Human Rights Act. The President of the Investigatory Powers Tribunal is Lord Justice Mummery, who previously acted as President of the Security Service and Intelligence Services Tribunals. Mr Justice Burton, the President of the Interception of Communications Tribunal, was appointed Vice-President of the Investigatory Powers Tribunal.

25. Complaints to the new Investigatory Powers Tribunal cannot be easily "categorised" under the old three Tribunal system. Consequently, it is not possible to detail those complaints to the Investigatory Powers Tribunal that related to the interception of communications that would have previously been considered by the Interception of Communications Act Tribunal. I can only provide information on the total number of complaints made to the new Investigatory Powers Tribunal (IPT). The new IPT received 11 new applications from the day of its formation on 2 October to the end of December 2000. Investigations into these complaints have been initiated although no case has been determined during this period. All the cases have been carried over to 2001.

Assistance to the Tribunal

26. Section 57(3) of RIPA requires me to give all such assistance to the Tribunal as the Tribunal may require in relation to investigations and other specified matters. Although Lord Justice Mummery, the President of the Tribunal, and I have consulted each other on matters of interest and concern to both of us, such as staffing, it has not been necessary for me to give to the Tribunal any assistance on the formal basis envisaged by the section.

Errors

27. A significant number of errors and breaches have been reported to me during the course of the year – 26 in all. By way of example, details of some of these are recorded below. It is important from the point of view of the public that I should stress that none of the breaches or errors were deliberate, that all were caused by human error or technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. The most common cause of error is a simple transposition of numbers by mistake, e.g. 3142 instead of 3124. The examples that I give are typical of the totality and are anonymous. Full details of the errors and breaches are set out in the confidential annex.

28. The Home Office reported a case concerning a warrant targeting an importer of class A drugs which was authorised by the Secretary of State on 27 March 2000 and subsequently renewed until 2 June 2000. However, three telephone numbers were deleted by HM Customs and Excise and a letter requesting the cancellation of the warrant was submitted dated 9 May 2000. An additional letter requesting the modification of the warrant was submitted by HM Customs and Excise dated 12 May 2000. The cancellation was amended to modification and signed by the Secretary of State on 31 May 2000. Because the warrant was originally due to be cancelled, HM Customs and Excise omitted the warrant from the bulk renewal report authorised by the Secretary of State on 31 May 2000 and unauthorised intercept took place between 2 and 6 June 2000. The breach appears to have occurred because of human error.

29. An error arose when a number of warrants needed to be cleared quickly through a Home Office senior official prior to their authorisation by the Secretary of State for Northern Ireland (who was acting as signatory on this occasion). Confirmation of the Secretary of State's signature allowed the Warrants Unit to convey details to the Public Telecommunications Operators (PTOs) to implement interception. However, it appears that one case that was telephoned through to the PTOs related to a case that had still to be signed off by the senior official. The PTOs were contacted immediately to request that interception be stopped. Of the two intercepts concerned only one had been set up; the other was in the process of being set up. No product was received on either line. This error was caused by human error and I am assured that, in future, appropriate tracking of files will be maintained.

30. The Security Service has reported an error which occurred when a transcriber reported two very short calls that appeared entirely unconnected as the two participants were in a different part of the country to the warranted target. The calls were not transcribed and the product was destroyed. Further research showed four similar earlier occurrences between the same individuals at the same time of day. In each instance the product was not transcribed and was immediately destroyed. Despite intensive investigation neither the Security Service nor the PTO have been able to determine the reason for the fault which led to these

unauthorised interceptions. The Security Service cancelled the warrant and reminded its staff of the importance of reporting promptly these faults so as to avoid a repetition.

31. The Security Service has reported three separate errors involving warrants containing incorrect telephone numbers; individual digits within the numbers either completely wrong or transposed incorrectly. On discovery, the intercepts were immediately suspended. In two cases, product was received but was destroyed before being transcribed. No product was received in the third and final case. The Security Service has acknowledged the importance of checking telephone numbers very carefully, especially during emergency applications and I have been assured that similar occurrences should not recur.

32. GCHQ has reported an error when 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. New procedures have been introduced which aim to detect further errors.

33. Another case involved the interception of a target whose telephone number was now registered in the name of another person. On discovery, the intercept was immediately stopped. A total of 66 conversations were intercepted although no transcripts or intelligence reports were produced. The shared nationality of the individual targeted in error and the wanted target contributed to the lengthy time for which this line remained intercepted. All traffic has been purged from GCHQ's working and archive databases. New procedures have been introduced which aim to detect further errors.

34. SIS reported an error which involved a warrant containing an incorrect telephone number; individual digits within the number were transposed incorrectly. On discovery, the intercept was immediately suspended. The material intercepted was not transcribed and has been destroyed. The original number has been deleted from the warrant and the correct number added. The mistake arose through human error. SIS has acknowledged the importance of checking telephone numbers very carefully.

35. An error reported by the Northern Ireland Office concerned a warrant in a batch of thirteen which had, inadvertently, not been signed by the Secretary of State. A copy of the instrument was faxed to the PTO who, on receipt, had "provided" for the line and interception commenced. It was only whilst routinely processing the paperwork on to a database that the PTO staff noticed that the Secretary of State had dated but not signed the warrant. The line was immediately suspended. A total of ten calls were intercepted although only one was transcribed. All product of this intercept has been destroyed.

36. Another case involved a modification adding two telephone numbers to a warrant. An error occurred in that two copies of the same modification were sent for signature by e-mail. Once signed the Communications Service Providers (CSPs) concerned were advised and asked to begin interception on the lines submitted for modification. At a later date it was realised that two of the modification instruments were identical. The CSP was contacted and the two lines suspended. There had been no calls on one of the lines. On the second line a total of ten calls had been intercepted and transcribed. The calls were deleted from the interception centre and all papers destroyed.

37. An error reported by Metropolitan Police Special Branch (MPSB) related to a police warrant application which mentioned the home telephone number of a target

on two occasions. In one section of the application the last two digits of the number had been transposed, through a simple typing error. The number was correctly recorded in the second section of the application. Home Office warrants unit staff noticed this mistake when the feasibility checks were repeated with the relevant telephone operator. MPSB was made aware of the error and confirmed the correct telephone number. However, the warrant signed by the Home Secretary contained the incorrect number. This was noticed when Home Office warrant staff provided initial notification to MPSB that the warrant had been signed. The telephone operator was immediately informed. No interception took place. The warrant was subsequently modified by deleting the incorrect number and adding the correct target telephone number.

38. HM Customs and Excise (HMCE) reported an error where an intercept for a telephone number was authorised as a modification to an existing warrant. HMCE was advised by the Home Office that the PTO had continued the interception of the telephone following the expiry of the warrant. It transpired that a request to extend the warrant had been inadvertently omitted from HMCE's monthly renewal application. The intercept was terminated immediately. Although there was a period of illegal interception, it transpired that no product had been received from this intercept because, in all probability, the target had disposed of this pre-paid mobile telephone. HMCE recognised that the error lay in their failure to include the warrant in the monthly renewal application although it should be noted that the PTO should have cancelled the intercept as they had not received a renewal instrument on expiry of the warrant. The incident has highlighted a lacuna in HMCE's system which they have remedied.

39. Another error related to a modification to an existing warrant. HMCE submitted an application to modify a warrant by adding a number. The modification instrument was authorised and interception commenced. However, it was immediately apparent that a person other than the target was using the telephone. On checking the interception details HMCE established that the number submitted on the modification application was incorrect in that one digit had been mistyped. The intercept was immediately terminated and the product was destroyed.

40. A case reported to me by the National Criminal Intelligence Service (NCIS) concerned a person reported missing by his family. The person's relative received a call seeking money for his return. This was reported to the police. The incoming telephone numbers were subsequently obtained and checked. The information revealed a call to the relative's number at about the same time, and that one of the names recorded on the register of voters matched an individual who had previously been involved in a kidnap investigation. NCIS made an emergency application for a warrant to intercept the telephone used by those thought to be holding the person. A warrant was issued. However, interception was suspended immediately it became apparent that the subscriber of the telephone was a relative of the missing person and not concerned in the alleged kidnapping. Although the interception period lasted for 1 hour 50 minutes, no calls were intercepted.

41. I turn to give examples of errors by PTOs.

42. One case involved two breaches of a telephone intercept warrant. The intercept on a target number was suspended as limited resources appeared to dictate that the Security Service would no longer be able to transcribe the product from the intercept. However, the intelligence section responsible for the particular investigation asked that the intercept be reinstated since transcription resources

could now be allocated to the intercept. As the warrant was extant, the PTO and the agency through which the traffic is routed to the Service were both contacted for this to be arranged. The desk officer responsible for the warrant then reported that a transcriber had heard unusual product from the intercept. The PTO concerned was informed about the problem and asked to investigate it. They were unable to explain it, but did mention another problem: when the intercept had been reinstated a mistake had been made at the routing agency and as a result product from an SIS warrant was passed to the Service. This product has since been destroyed. Investigation by the Service showed that the owner of the telephone was aware of the problem mentioned above. But it is thought that the problem was caused by an engineering fault, and was unconnected to the Service's intercept.

43. The Secret Intelligence Service reported two interception errors made by Communications Service Providers (CSPs). One case involved a warrant covering a target involved in the large-scale importation of heroin and cocaine into the United Kingdom. Whilst trying to locate a network problem, PTO staff inadvertently routed product to SIS in addition to the product customer, HM Customs and Excise. This breach appears to have occurred because of technical errors made by PTO staff who subsequently informed the appropriate Agencies of the problem. The PTO has now modified the exchange software to prevent a recurrence of this problem.

44. The other case concerned what appeared to be non-target traffic appearing on a line covered by the warrant. The line was suspended pending further investigation. The investigation showed that this was caused by a technical problem which was immediately cured and will not recur. In fact by the time that the nature of the fault was discovered SIS had decided to cancel the warrant on operational grounds. The product from these calls was not transcribed and SIS deleted all the calls from their system. As already indicated in paragraph 27 in each case where an error has occurred and interception has taken place the product was destroyed on discovery of the error.

Conclusion

45. The interception of communications is, as my predecessors have expressed in their Reports, an invaluable weapon for the purpose set out in section 5(3) of RIPA and, in particular, in the battle against serious crime. The task of the Agencies working in this field has become much more difficult and complex as a result of the proliferation of mobile telephones and the greater sophistication of criminals and terrorists. RIPA brought the legislation up to date in the light of new developments in technology in the communications industry, such as e-mail, satellite telephones, radio pagers and the like and the proliferation of mobile telephones. An individual warrant may permit the interception of the person named in the warrant or named premises. The law was simplified in relation to the implementation of warrants, the issue of emergency warrants, their duration and their discharge. These changes have increased the efficiency of the enforcement agencies and the speed with which, in appropriate circumstances, they may act but in each case they are covered by section 15 safeguards.

Statistical Annex to the Report of the Commissioner for 2000

Warrants (a) in force, under Interception of Communications Act 1985, on 1 October 2000 and (b) issued during the period 1 January 2000 to 1 October 2000

	<i>Telecommunications</i>		<i>Letter</i>		<i>Total</i>
	a	b	a	b	
Home Secretary	446	1425	26	49	1474
Scottish Executive	67	237	0	0	237

Warrants (a) in force, under Regulation of Investigatory Powers Act 2000, on 31 December 2000 and (b) issued during the period 2 October 2000 to 31 December 2000

(NB: Under Regulation of Investigatory Powers Act 2000 there is no longer a breakdown of the figures between Telecommunications and Letters)

	a	b
Home Secretary	555	606*
Scottish Executive#	32	55

*This figure includes 472 IOCA warrants that were revalidated as RIPA warrants on the coming into force of Regulation of Investigatory Powers Act 2000 on 2 October 2000.

In July 1998 a new policy was implemented whereby the section 5 power to modify warrants was to be extended to serious crime warrants. The total figures for modifications are as below:

IOCA (1/1/00 – 1/10/00)	488
RIPA (2/10/00 – 31/12/00)	234

Scottish Executive

Under RIPA the Secretary of State for Scotland was initially empowered to sign warrants. An Executive Devolution Order dated 13 December 2000 transferred this power back to the Scottish Ministers.

Interception of Communications Act 1985: 1/1/2000 – 30/9/2000

The First Minister and Deputy First Minister authorised warrants for 235 serious crime cases and two HM Customs' cases.

Regulation of Investigatory Powers Act 2000 Part I: 1/10/2000 – 31/12/2000

The Secretary of State for Scotland and the First Minister authorised warrants for 53 serious crime cases and two HM Customs' cases.

The comparative figures for 1999 are 288 warrants signed, comprising 231 serious crime cases, 44 HM Customs' cases and 13 for terrorism (following Devolution, no national security cases have been authorised by Scottish Ministers since 1 July 1999).

