Report of the Interception of Communications Commissioner for 2002

Commissioner:
THE RT HON SIR SWINTON THOMAS

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
9 September 2003

Laid before the Scottish Parliament
by the Scottish Ministers
September 2003

HC 1047
SE/2003/210

£5.00

Report of the Interception of Communications Commissioner for 2002

Commissioner:
THE RT HON SIR SWINTON THOMAS

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
9 September 2003

Laid before the Scottish Parliament
by the Scottish Ministers
September 2003

HC 1047
SE/2003/210

Contents

Subject	*Page*
Letter to the Prime Minister	iv
Introduction	1
Functions of the Commissioner	1
Discharge of my functions	1
The extent of interception: General	4
Safeguards	4
Codes of Practice	5
Communications data	5
Prisons	5
Foreign and Commonwealth Office and Northern Ireland Office Warrants	6
The Investigatory Powers Tribunal	7
Assistance to the Tribunal	7
Errors	7
Conclusion	11
Statistical Annex	12

From: The Right Honourable Sir Swinton Thomas

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

30 April 2003

I enclose my third 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the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published.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 2001

Introduction

1. I was appointed the Interception of Communications Commissioner on 11 April 2000 under the provisions of the Interception of Communications Act 1985, and as from 2 October 2000 under section 57 of the Regulation of Investigatory Powers Act 2000. This is my third annual report as Commissioner and covers the year ending 31 December 2002.

2. My three-year appointment as Interception of Communications Commissioner expired on 10 April 2003. However, following an invitation from the Prime Minister I have accepted reappointment as the Interception Commissioner for a further three years until 10 April 2006.

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 that cannot be fully explained without disclosing sensitive information relating to particular agencies or to individuals concerned are contained in the Confidential Annex.

Functions of the Commissioner

4. The coming into force of the Regulation of Investigatory Powers Act 2000 (RIPA) on 2 October 2000 coincided with the coming into force of the Human Rights Act 1998 (HRA) which incorporated the European Convention on Human Rights into UK law. It is right to emphasise that these two important pieces of legislation brought about a number of changes in the law and in the practice of those responsible for the lawful interception of communications.

5. My functions as Commissioner are set out in section 57 of the Act and are as follows:

- To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 7 to 11 of RIPA and the adequacy of any arrangements made for the purpose of sections 15 and 16 of RIPA.

- To keep under review the exercise and performance by the Secretary of State of the powers and duties conferred or imposed by or under Chapter II of Part I (the acquisition and disclosure of communications data).

- To give the Investigatory Powers Tribunal set up under 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 31 to 33 below.

Discharge of my functions

6.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 power 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 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.

7. In accordance with these duties I have continued my practice of making twice yearly visits to the Security Service, the Secret Intelligence Service, GCHQ, the National Criminal Intelligence Service, the Special Branch of the Metropolitan Police, Strathclyde Police, the Police Service for Northern Ireland, HM Customs and Excise, the Foreign and Commonwealth Office, the Home Office, the Scottish Executive and the Ministry of Defence. Prior to each visit I obtain a complete list of warrants issued or renewed since my previous visit. I then select, largely at random although there have been occasions where I have indicated specific cases that I want to see, a sample of warrants for close inspection. In the course of my visit I satisfy myself that the warrants fully meet the requirements of RIPA, that proper procedures have been followed, that the relevant safeguards and codes of practice have been followed. During each visit I review each of the files and the supporting documents and discuss the cases directly with the operational officers concerned. I can view the product of interception. It is important to ensure that the facts justify the use of interception in each case and those concerned with interception fully understand the safeguards and the codes of practice.

8. I have been very impressed by the quality, dedication and enthusiasm of the personnel carrying out this work on behalf of the government and the people of the United Kingdom. They show that 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. All errors are reported to me and if there is any product it is immediately destroyed. In conforming to the statutory duty placed on them, the agencies have made available to me everything that I have wished to see or hear. 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 the agencies' anxiety to comply with the law. In a case of doubt or difficulty, they do not hesitate to contact me.

9. During the year I have also seen the Home Secretary, the Foreign Secretary, the Secretary of State for Northern Ireland, the Secretary of State for Defence and the First Minister for Scotland. I have been impressed with the

care that they take to satisfy themselves that the warrants are necessary for the authorised purposes. If the Secretary of State has any doubts about the application and is minded to refuse it, further information or clarification would be sought so that reconsideration is given to issuing or renewing a warrant. Outright refusal of an application is comparatively rare because of the care with which applications are prepared by the agency concerned and scrutinised by the senior officials in the Secretary of State's department before they are submitted to him. However, I view the occurrence of occasional outright refusals, where for example, the strict requirements of necessity and proportionality are not met in the opinion of the Secretary of State, as a healthy sign. It shows that the Secretaries of State do not act as a "rubber stamp".

10. During 2002 I also visited the communications service providers (CSPs), that is to say the Post Office and major telephone companies. Each of the CSPs employs personnel who are engaged solely on the execution of interception of communications warrants. They have acquired 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 sensitive area and with their understanding of the need at all times to comply with the safeguards imposed on them.

11. During the course of the year I attended, together with the Intelligence Services Commissioner, upon the Intelligence and Security Committee's Conference Dinner and, on separate occasions, upon the Australian Inspector-General and the Secretary to the Joint Intelligence Committee, to discuss matters of mutual interest and concern.

12. I also met, without the Intelligence Services Commissioner, the Director of Public Prosecutions and the Director of Casework at the Crown Prosecution Service to discuss legal issues associated with RIPA. In addition I was briefed by the new National Technical Assistance Centre (NTAC) on its history, aims and functions and I provided them with some observations on their draft safeguards document, which they were happy to accept.

13. In February 2002, at the request of the Secret Intelligence Service (SIS), I paid a short visit to Jamaica, Barbados, and Trinidad to discuss the question of legislation governing the interception of communications with representatives of the governments, senior officials, members of the judiciary and others in those countries. I believe that this visit was welcomed and fruitful. It was followed up successfully by members of the legal department of SIS.

14. In my Report last year I highlighted the possible suspicions that some members of the public may have that their telephone conversations are being unlawfully intercepted by the security, intelligence or law enforcement agencies. Through all aspects of my oversight work I am as satisfied as it is possible to be that deliberate unlawful interception of communications of the citizen does not take place. I say "deliberate" because on rare occasions technical errors do occur which may render an interception unlawful in which case the product, if any has been received, from the interception is always destroyed.

15. By law, the interception of an individual's communications can take place only after a Secretary of State has granted a warrant and the warrant can be granted on strictly limited grounds as set out in section 5 of RIPA, essentially in the interests of national security and the prevention and detection of serious crime. Of course, it would theoretically be possible to circumvent this procedure, but there are extensive safeguards in place to ensure that this cannot happen, and I am satisfied that it does not. I consider it an important part of my oversight role to ensure that these safeguards are in place and that they are observed.

16. In previous years my annual report has received some, albeit not extensive, coverage in the press. This reporting has concentrated almost exclusively on my references to errors which have taken place in the course of the year as opposed to the many positive aspects of my report. I think that this is a pity, bearing in mind that the positive aspects of my report so far outweigh the negative aspects.

The Extent of Interception: General

17. As in the past, the Annex to this Report contains a summary of the numbers of warrants in force at the end of 2002 and those issued throughout the course of the year by the Home Secretary 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 significantly high level of warrants sought each year, with a corresponding level of workload for the Secretaries of State and on the part of the relevant agencies, clearly calls for the exercise of vigilant supervision. I can report that the level of scrutiny has been, and continues to be, generally well maintained. Although the number of errors reported to me during 2002 is slightly lower than that recorded in my Report last year, I still remain concerned about its level. It is inevitable that in any detailed, technical human activity errors may occur. Nevertheless I have impressed on the agencies the need to eliminate errors or, at least, to reduce them to an absolute minimum. The agencies are very aware of the importance of this, and on each occasion where an error has occurred they review their procedures with a view to ensuring that the same error does not recur. Keeping errors to a minimum is one of the reasons for having safeguards in place. 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 if they do.

Safeguards

18. 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 the dissemination, disclosure, copying, storage and destruction etc., of intercepted material. These sections of the legislation require careful and detailed safeguards to be drafted by each of the agencies and for those safeguards to be approved by the Secretary of State. This has been done. As I mentioned in my last Report I have been impressed by the care with which these documents have been drawn up. My advice and approval was sought for the documents and I am approached to agree amendments to the safeguards when they are updated in light of technical and administrative developments.

19. During 2002 the Home Office began working on updating the Handbook for Communication Service Providers (CSPs). I contributed to this process by providing both a few suggested guidelines on what should be covered in the section on safeguards and advice on the obligations that should be placed on the CSPs for the purpose of facilitating my carrying out of the functions as Commissioner.

20. I cannot emphasise enough that the sections 15 and 16 requirements are very important. Those involved in the interception process are well aware of the invasive nature of this work and care is taken to ensure that intrusions of privacy are kept to the minimum. I am satisfied that the agencies are operating effectively within their safeguards.

Codes of Practice

21. Section 71(2)(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 Interception of Communications Code of Practice, on which the Home Secretary obtained my views, was published during 2002.

22. During the course of the year I was also asked by, and I duly provided, the Home Office with my views on the draft Code of Practice relating to Part III of RIPA — encryption keys.

Communications data

23. Chapter II of Part I of RIPA applies to the acquisition and disclosure of communications data. Section 57 of the Act requires me to keep under review the exercise and performance by the persons on whom they are conferred or imposed these powers and duties. Chapter II of Part I is not yet in force. A draft Order adding a number of additional public authorities to the RIPA access to communications data provisions was laid before Parliament in June 2002. However, following controversy in Parliament and elsewhere, the Home Secretary decided to withdraw the RIPA Order to allow for wider consultation on the issue. As part of this consultation process I had a very useful meeting in November 2002 with the consultants appointed by the Home Secretary to the communications data review group.

24. At the end of the full consultation exercise new proposals will be brought forward on access to communications data and a new Order placed before Parliament. It is anticipated that this will be done before Parliament rises for the summer recess in July 2003 with implementation occurring by the end of 2003.

25. The delay in bringing into force Part I Chapter II is well documented. However, I have to report the ongoing concerns expressed to me by the agencies of the failure to implement this part of the legislation and its relevant Code of Practice. I understand that this problem is compounded by real difficulties in implementing Part 11 of the Anti-Terrorism, Crime and Security Act regarding retention of data. Until these communications data issues are resolved Part III of RIPA — investigation of electronic data protected by encryption — is unlikely to be addressed.

Prisons

26. In paragraph 59 of my report last year, I highlighted the fact that I had been asked by the Home Secretary to oversee the interception of communications in prisons for police and security purposes. Although this function does not fall within my statutory jurisdiction under RIPA, I agreed, in principle, to undertake this role given my experience of, and responsibility for, the interception of communications under that legislation. I have now had the opportunity to undertake familiarisation visits to five establishments—HM Prison Belmarsh, HM Prison High Down, HM Prison and Young Offenders Institution Doncaster, HM Young Offenders Institution and Remand Centre Glen Parva and HM Young Offenders Institution and Remand Centre Feltham.

27. At all the establishments there were three primary areas of inspection:

- The methods utilised in the establishments for the interception of telephone communications and postal communications.

- A physical inspection of the interception of telephone communications and the equipment utilised.

- A physical inspection of the arrangements for the interception of postal communications.

28. I was particularly concerned to ensure that all interception was carried out lawfully and in accordance with the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, and the Prison Rules made under the Prison Act 1952. Insofar as the Human Rights Act and Regulation of Investigatory Powers Act 2000 are concerned the primary responsibility for compliance with the legislation lies with the police force making an application for the disclosure of information obtained by means of interception.

29. After each visit I produced a brief individual report for the prison Governor and Prison Service Headquarters detailing my findings. I do not propose to go into any detail about these visits, or my findings, in this Annual Report. However, it is worth mentioning that my overall impression following the five visits is that the arrangements of interception in the establishments inspected has highlighted a number of inconsistencies in the approach to interception work in prisons, and that the Prison Rules are not always strictly complied with. These are issues that will need to be addressed by the Prison Service.

Foreign and Commonwealth Office and Northern Ireland Office warrants

30. In paragraphs 10—12 of my predecessor's 1995 Annual 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 again to emphasise the important reasoning behind this decision.

31. 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 the 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."*

32. 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 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 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 to this Report.

The Investigatory Powers Tribunal

33. The Investigatory Powers Tribunal (the Tribunal) was established by section 65 of the Regulation of Investigatory Powers Act 2000. The Tribunal came into being on 2 October 2000 and from that date 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 Tribunal is Lord Justice Mummery with Mr. Justice Burton acting as Vice-President. In addition, seven senior members of the legal profession serve on the Tribunal. A Registrar has also been appointed to help in the process of hearing claims alleging infringements of the Human Rights Act.

34. As I explained in paragraph 25 of my first Annual Report in 2000, complaints to the Tribunal cannot easily be "categorised" under the three Tribunal system that existed prior to RIPA. Consequently, I am unable to detail those complaints that relate solely to the interception of communications. I can only provide the information on the total number of complaints made to the Tribunal. The Tribunal received 130 new applications during 2002 and completed its investigation of 67 of these during the year as well as concluding its investigation of 27 of the 31 cases carried over from 2001. 67 cases have been carried forward to 2003. On no occasion has the Tribunal concluded that there has been a contravention of RIPA or the Human Rights Act 1998.

Assistance to the Investigatory Powers Tribunal

35. 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. I was not asked to assist the Tribunal during the year 2002.

Errors

36. A significant number of errors and breaches have been reported to me during the course of the year—39 in all. Although slightly lower than the total for 2001, the number is still unacceptably high. By way of example, details of some of these errors and breaches are recorded below. It is very important from the point of view of the public that I stress that none of the breaches or errors were deliberate, that all were caused by human or procedural error or by 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 tends to be the simple transposition of numbers by mistake e.g., 1809 instead of 1890. 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.

37. Two errors occurred at the Home Office. The first occurred when the Home Office received a request to cancel a warrant when in fact the agency concerned only required certain addresses to be deleted from the schedule by modification deletion. The warrant had two other live schedules in operation for other communications service providers (CSPs). Home Office checks should have shown that the warrant had these other extant lines but due to human error this was overlooked. Therefore although the warrant was cancelled the address remained active with the other CSPs. When it was established that a cancellation instrument had been signed erroneously as a result of the requesting agency's letter being misinterpreted at the Home Office all interception with the CSPs was suspended and the agency instructed to apply for a new warrant against the target.

38. The second error related to a mobile telephone number added to an existing warrant under the urgent procedures. Although the intercepting agency sent the ratification to the Home Office before its expiry date, Home Office officials failed to have the ratification signed by a senior official before the expiry date. Once the error was noticed by the Home Office the intercept was immediately suspended until a new modification was added to the warrant. Whilst I understand the difficulties that may be encountered by the intercepting agencies and warrant-issuing departments, particularly during a holiday period, I do consider it unsatisfactory that an error should occur as a result of an urgent modification expiring before it is signed.

39. One error was reported by the Scottish Executive although the fault for the error lies, not with them, but with a Scottish police force. The police force sought, and obtained, from the Scottish Executive a warrant, which was signed on 8 August 2002. By 13 August 2002 it became apparent that the intercept was not producing any intelligence. It transpired that the telephone number on the interception warrant was incorrect by one digit. Investigations revealed that the intelligence records in respect of the target showed the correct telephone number but that a mistake occurred within the police force when the number was transcribed into the warrant application form to the Scottish Executive.

40. The Northern Ireland Office reported an error in a warrant signed by the Secretary of State for Northern Ireland although the error itself occurred in the paperwork presented to Northern Ireland Office officials by the mainland police force seeking the warrant. Investigations revealed that a police officer in the mainland force incorrectly transferred details of the target's telephone number from his written notes to the warrant application form; two digits in the communications address became transposed. Unfortunately, due to the urgent nature of the application it was submitted, via NCIS, with the error intact.

41. Seven errors were reported by GCHQ of which three are highlighted below. In the first case the intercept product revealed that the user was no longer the target but a new subscriber. An immediate subscriber check with the CSP confirmed that the user had indeed changed and the intercept was immediately ceased. The error occurred as a result of a reallocation of the telephone number. GCHQ's discussions with various CSPs highlighted the short term difficulties that the network providers had in tracking the reallocation of numbers within their customer databases.

42. The second error occurred as a result of a typing error within GCHQ. A modification was made to an existing GCHQ warrant and once the signature had been confirmed, the CSP were e-mailed with instructions to provide intercept of the relevant telephone numbers. Unfortunately, the member of staff at GCHQ who sent the e-mail mistyped three of the digits. When the CSP

received their copy of the signed modification they realised an error had been made; they cancelled the wrong line immediately. No calls had been intercepted. GCHQ has modified its internal working arrangements to prevent a recurrence.

43. The third case involved a GCHQ warrant that was issued by a senior official at the Foreign Office on the authority of the Secretary of State in accordance with Section 7(4) of RIPA. The warrant was subsequently renewed by the Secretary of State. Before the renewal of the warrant an urgent modification to add a further telephone number to the schedule was authorised by the Director of Operations at GCHQ and was valid for five working days. Although the warrant was renewed the modification should have been submitted to the Foreign Office for approval before its expiry (it expired two days after the renewal was signed). This administrative procedure was overlooked and was not discovered until five days after the renewal instrument was signed. A modification to add the number was then duly approved by the Foreign Office. All the calls intercepted during this unauthorised period have been destroyed.

44. The Security Service reported fourteen errors. Eight of the fourteen errors related to breaches of the Security Service's arrangements for handling intercepted material. Five of these breaches occurred when the Security Service judged it necessary for GCHQ to transcribe product from these five separate warrants because of the linguistic resources required. Unfortunately the relevant desk officers responsible for the warrants were not aware that it was necessary to seek the agreement of the Security Service's Deputy Director-General for the product to be transcribed by GCHQ and the product was passed without that authorisation. I understand that Security Service staff have been reminded of the requirement to seek the necessary authorisation before passing raw or undisguised product outside the Security Service. These breaches are somewhat technical, and there is no doubt that the Deputy Director-General would, if asked, have given the necessary authorisation. This, perhaps, emphasises the stringent criteria rightly applied by the Agencies in reporting errors to me.

45. The circumstances surrounding the sixth breach of the Service's handling arrangements are exactly as that reported in the preceding paragraph except this breach was compounded by the Security Service's desk officer's failure to issue GCHQ with a caveat advising that no further dissemination should be given to the product nor use made of it without prior reference to the Security Service. In the absence of such a caveat GCHQ assumed that it was for it to report the intercepted calls and so issued a number of reports. The material was, of course, handled and reported in accordance with GCHQ's own rigorous security procedures. Security Service staff have been reminded of the requirement to seek not only the necessary authorisation before passing raw or undisguised product outside the Security Service but also of the need to include an appropriate caveat when doing so.

46. The seventh handling breach occurred when a desk officer in the Security Service passed undisguised product from an interception warrant to the Department of Trade and Industry (DTI). The product was retrieved a couple of days later when the mistake was noticed. The appropriate authorisation was subsequently sought to pass the undisguised product to the DTI.

47. The eighth, and final, handling breach relates to the disclosure of legally privileged material that occurred in connection with one of the Security Service's interception warrants. Intelligence was passed without the specific protective handling caveats which are given to intercepts of legally privileged communications on the prior approval of a Security Service legal adviser to an

officer at HM Customs and Excise working on the operation. I understand that Security Service staff have now been reminded of their responsibilities in handling legally privileged material

48. The ninth error occurred when a warrant contained an incorrect telephone number; individual digits within the number being transposed incorrectly. On discovery, the unlawful intercept was suspended and the copies of all the relevant transcriptions destroyed.

49. The reasons for the remaining five errors occurring were the Security Service's failure to cancel a warrant imposed under emergency procedures prior to its expiry date; their incorrect request to delete both lines covered by a warrant and not just the line they intended; their failure to request the deletion of a number from a warrant and the failure to subsequently cancel the warrant itself; and their using an incorrect postcode in an emergency modification to a warrant.

50. The Secret Intelligence Service (SIS) reported one breach and two errors. The breach and first error occurred under one submission. The breach arose from a mistake by a SIS operational team member which resulted in transposed digits in the telephone number being used in the warrant application. The error resulted from the use of what subsequently turned out to be an out-of- date number given to SIS by the Security Service from a departmental file. My view is that it would be unreasonable to blame SIS for being given, and acting on, wrong information.

51. The second error occurred through a lapse in SIS's internal procedures. The late cancellation of an intercept with a CSP resulted in interception of a number continued for one day after the deletion instrument relating to that number had been signed. SIS has reviewed their procedures and taken steps to prevent a reoccurrence of a similar lapse.

52. HM Customs and Excise (HMCE) reported one error. It occurred when a modification was made to a schedule adding a telephone number to the warrant. Unfortunately the telephone number in the schedule included one incorrect digit. No product had been received and HMCE staff were duly reminded of the importance of their checking procedures

53. No errors were reported by the Ministry of Defence, Metropolitan Police Special Branch and the National Criminal Intelligence Service.

54. I now turn to give two examples of the ten errors made by the communications service providers (CSPs). The first occurred under a Scottish Executive warrant. The Scottish Executive advised the appropriate CSP of the telephone number to be intercepted but the CSP mistakenly transposed two digits in the number. Since the error occurred, the CSP concerned has reviewed its procedures to prevent a similar recurrence in the future.

55. The second example concerns a wrongly intercepted telephone number. A CSP received a verbal warrant modification request to intercept a mobile number. Their hand written records show that details of the number to be intercepted were correctly recorded at that time and a feasibility check confirmed the correct target. The details of the target were then entered into the CSP's operational database. It was at this stage that a human error occurred in that the penultimate digit was incorrect input. No calls were intercepted during the period of this illegal interception.

Conclusion

56. As I highlighted in my Report last year, the interception of communications is an invaluable weapon for the purpose set out in section 5(3) of RIPA and, in particular, in the battle against terrorism and serious crime. The task of the agencies working in this field has become 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. 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 whilst in each case being covered by section 15 safeguards.

57. It is my view that in 2002, as before, interception played a vital part in the battle against terrorism and serious crime, and one that would not have been achieved by other means. I am also satisfied that Ministers and the intelligence and law enforcement agencies carry out this task diligently and in accordance with the law.

Annex to the report of the Commissioner for 2002

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2002 and (b) issued during the period 1 January 2002 and 31 December 2002

	a	b
Home Secretary	515	1466
The total number of RIPA modifications from 01/01/2002 - 31/12/02 = 1885		
Scottish Executive	40	139
The total number of RIPA modifications from 01/01/2002 - 31/12/02 = 258		

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

Printed in the UK for The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
09/03 065536 ID 150908

Published by TSO (The Stationery Office) and available from:

Online
www.tso.co.uk/bookshop

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Fax orders 0870 600 5533
Order through the Parliamentary Hotline *Lo-call* 0845 7 023474
Email book.orders@tso.co.uk
Textphone 0870 240 3701

TSO Shops
123 Kingsway, London WC2B 6PQ
020 7242 6393 Fax 020 7242 6394
68-69 Bull Street, Birmingham B4 6AD
0121 236 9696 Fax 0121 236 9699
9-21 Princess Street, Manchester M60 8AS
0161 834 7201 Fax 0161 833 0634
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
18-19 High Street, Cardiff CF10 1PT
029 2039 5548 Fax 029 2038 4347
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/General enquiries 020 7219 3890
Fax orders 020 7219 3866

TSO Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0-10-292329-9

9 780102 923292