
Report of the Interception of Communications Commissioner for 2003

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
22 July 2004

Laid before the Scottish Parliament
by the Scottish Ministers
July 2004

Report of the Interception of Communications Commissioner for 2003

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
22 July 2004

Laid before the Scottish Parliament
by the Scottish Ministers
July 2004

Contents

<i>Subject</i>	<i>Page</i>
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
Communications data	4
Prisons	5
Foreign and Commonwealth Office and Northern Ireland Office Warrants	6
The Investigatory Powers Tribunal	6
Assistance to the Tribunal	7
Errors	7
Conclusion	10
Statistical Annex	11

From: The Right Honourable Sir Swinton Thomas

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

17th May 2004

Dear Prime Minister,

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the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published.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

*Yours sincerely,
Swinton Thomas*

Sir Swinton Thomas

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

Annual Report of the Interception of Communications Commissioner for 2003

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. At the invitation of the Prime Minister I have been re-appointed as the Interception of Communications Commissioner until 10 April 2006. This is my fourth annual report as Commissioner and covers the year ending 31 December 2003.

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 concerned are contained in the Confidential Annex.

Functions of the Commissioner

3. 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.

4. 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 27 to 29 below.

Discharge of my functions

5. 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 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 came into force on 5 January 2004. Part III is not yet in force.

6. In accordance with these duties I have continued my practice of making twice yearly visits to the Security Service, the Secret Intelligence Service, Government Communications Headquarters, 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, and 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.

7. I have been 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 more detail in the Confidential Annex) these have been errors of detail or procedure 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, and to seek advice.

8. During the year I have also seen the Home Secretary, the Secretary of State for Northern Ireland, the Secretary of State for Defence and the First Minister for Scotland. It is clear to me that each of them gives a substantial amount of time and takes considerable care to satisfy himself or herself that the

warrants are necessary for the authorised purposes, and that what is proposed is proportionate. If the Secretary of State wishes to have further information in order to be satisfied that he or she should grant the warrant then it is requested and given. Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity or proportionality are not met, and the agencies are well aware that the Secretary of State does not act as a "rubber stamp".

9. During 2003 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 responsible for 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. The CSPs have a vital role to play in this field, and I am sure that it is of first importance, if any change in the law is proposed which may affect them and their staff, that they should be consulted and their views and concerns taken into account.

10. On 12 May 2003 I gave evidence to Mr Justice Butterfield in relation to his enquiry to review current practices and procedures relating to the disclosure, associated investigation techniques and case management in HM Customs and Excise's criminal cases.

11. In May 2003 I was sent an updated copy of the GCHQ compliance documentation, and asked to approve it which I did: it is through the measures described in this documentation that the safeguards referred to in RIPA paragraphs 17 – 18 are maintained.

12. In September and November 2003 I visited two GCHQ facilities and inspected the work relevant to my role as Commissioner. I had the opportunity to see at first hand the work carried out at both sites, to talk to those in charge and to a number of staff. The visits were extremely informative and enabled me to see GCHQ's interception process in the round. I observed how the work is monitored, and I was satisfied that the relevant safeguards are being complied with. The work being done at both sites is invaluable for the purposes set out in section 5(3) of the Act.

13. In November 2003 I met, through the offices of the Intelligence and Security Committee, members of the German G10 Kommission to discuss matters of mutual interest and concern in the area of interception.

14. In my past Reports I have 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 continuing 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, the prevention and detection of serious

crime and safeguarding the economic well-being of the United Kingdom. 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.

The Extent of Interception: General

16. As in the past, the Annex to this Report contains a summary of the numbers of warrants in force at the end of 2003 and those issued throughout the course of the year by the Home Secretary and the First Minister in Scotland. 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 2003 is the same as 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

17. 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. 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.

18. The requirements of sections 15 and 16 of RIPA are vital. 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.

Communications data

19. 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 these powers and duties are conferred or imposed. The delay in bringing into force Chapter II of Part I is well documented. The Regulation of Investigatory Powers (Communications Data) Order 2003 was made on 5 December 2003 and came into force on 5 January 2004 (Statutory Instrument 2003 No. 3172), and so falls outside the scope of this Annual Report.

20. Both in the run up to, and following the Order coming into force I had numerous meetings with officials at the Home Office on establishing the appropriate oversight regime for the provisions of the Order. I am pleased to say that, following discussions with the Home Office, and in accordance with section 57(7) of RIPA, arrangements are now being put in hand to recruit additional staff to help me in my oversight of RIPA Part I Chapter II as well as my non-statutory role of overseeing interception in prisons (see paragraphs 21 – 25 below).

Prisons

21. In my earlier Annual reports, 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. In paragraph 26 of my 2002 report I detailed the first five establishments that I had visited. Since then I have re-visited HM Prison Belmarsh and made first time visits to HM Prison Wormwood Scrubs, HM Prison Lincoln, HM Prison Woodhill and HM Prison Nottingham.

22. My purpose in re-visiting HM Prison Belmarsh was to establish whether the deficiencies highlighted in my first visit had been addressed. Not all these had been and a report will be sent to the Governor concerning these.

23. At the other four 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.

24. 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. When interception in prisons is carried out on behalf of the police in the course of an investigation, then the primary responsibility for complying with the legislation lies with the police. When it is carried out on behalf of the prison authorities under the Prison Act and the Rules made under the Act, then the responsibility for compliance lies with the prison.

25. 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, my overall conclusion following these visits is that the arrangements for 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 which are being addressed by the Prison Service and must continue to be addressed.

Foreign and Commonwealth Office and Northern Ireland Office warrants

26. 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 to emphasise again the reasoning behind this decision.

27. 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."

28. 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

29. 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.

30. 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 109 new applications during 2003 and

completed its investigation of 43 of these during the year as well as concluding its investigation of 57 of the 67 cases carried over from 2001/2002. 76 cases have been carried forward to 2004. 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

31. 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 2003.

Errors

32. A significant number of errors and breaches have been reported to me during the course of the year – 39 in all. Although the level of errors is the same as that in 2002, 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.

33. The Home Office reported, on behalf of the National Technical Assistance Centre (NTAC), a breach of RIPA by a communications service provider (CSP), brief details of which are recorded later in this report under the CSPs.

34. The Scottish Executive reported to me an erroneous termination of an intercept and several other errors by CSPs that arose in their cases, brief details of which are recorded later in this report under the CSPs.

35. The Northern Ireland Office reported one error that occurred in a modification instrument to an interception warrant. The modification sought to add a new mobile telephone number to a warrant. Unfortunately, the mobile telephone number cited on the modification was that of a serving police officer and not a number used by the target. The interception was immediately ceased. The incorrect telephone number was deleted from the warrant and the correct number added.

36. Seven errors were reported by GCHQ of which three are briefly highlighted below. The first case concerns the need to remove four telephone numbers from a warrant. There is a due process in place that ensures that the deletion of numbers and cessation of interception occurs promptly. Unfortunately, a step in this process was overlooked and a check sheet, which should ensure that all steps in the process are followed, was not used. Consequently, the numbers continued to be intercepted. The product from the unauthorised intercepted calls has been destroyed. To prevent a recurrence, staff within GCHQ have been rebriefed on the necessity of using the check sheet to ensure all steps in the modification process are followed.

37. The second case involves avoidable human error: a transcriber failed to take the appropriate action when the circumstances of a target changed. This led to the unauthorised interception of three calls. These have been deleted and the relevant staff reminded of their responsibilities in ensuring the correct procedures are followed in similar cases.

38. The third case arose out of a technical fault in the computer system. At the same time that technical work was being undertaken to remedy a fault in the database, a GCHQ analyst made an entry on the database for a specific action to be carried out. Unfortunately the technical work had a subsequent adverse effect on the accuracy on the working of the database. I understand that technical faults of the kind that occurred are extremely rare and it was very unfortunate that it occurred at the same time as the analyst making an entry. This coincidence of events is very unlikely to happen again.

39. The Security Service reported eleven errors, brief details of six of these are highlighted below. Errors were reported in two separate cases where, although the warrants were properly obtained against the targets, product revealed that the telephone numbers quoted on the two warrants were incorrect and that the phones were not, in fact, being used by the intended targets.

40. The third error occurred in a case where warrants were obtained against two targets but the investigating officer had inadvertently transposed telephone numbers and targets on the individual warrants so that the interception warrants had the targets names on them with the other target's telephone number. It is vitally important that telephone numbers on warrants are checked very carefully. The Security Service has reviewed its procedures in the light of this error and has introduced a more rigorous system of double-checking numbers.

41. In the fourth case, the Security Service obtained a warrant with a mobile telephone number and a business landline number provided by the National Crime Squad who themselves were provided the numbers by a covert human intelligence source. It transpired that the mobile number was incorrect in that one digit was different. No product was received from this interception.

42. The fifth error occurred when the Security Service omitted to request the cancellation of a warrant. The Service recognise that this was as a result of human error despite the use of an IT system intended to help ensure the effective detailed control of the warrant process. The Security Service are considering how their procedures can be improved to prevent a recurrence of a similar error in the future.

43. The sixth error occurred when a warrant contained an incorrect telephone number: individual digits within the number being transposed incorrectly. No product from the line was listened to as the transcriber dealing with the case recognised the mistake immediately and suspended the line. The line was cancelled and the correct telephone number added to the warrant.

44. The reasons for the remaining five errors occurring include the opening by a CSP of a letter not covered by an interception warrant; the failure of both the Security Service's and a CSP's system to cancel intercepted lines and the Security Service intercepting a target's address which was then discovered to be slightly different from that quoted on the relevant warrant.

45. The Secret Intelligence Service (SIS) reported one error after they discovered that a mobile telephone number had been retained on a warrant for a period of time after the line had been disconnected by the operator. The line was immediately suspended on SIS's system and they initiated a warrant modification to delete the number from the warrant. Although the mistake was partly due to misinformation they had received from a CSP, SIS have taken immediate steps to ensure that their working processes are updated to prevent a recurrence of a similar error. As the line had been disconnected of course no communications were in fact intercepted after disconnection.

46. The Metropolitan Police Special Branch (MPSB) reported three errors to me. All three errors relate to the late cancellation of interception warrants in respect of three separate operations. In all three cases the CSPs were instructed to cease interception; however, MPSB failed to make a prompt application to the Home Office to seek cancellation of the three warrants. MPSB have acknowledged that their failure to act was due to human error and a lack of robustness in their current operating systems. I have been assured that systems have been put in place to ensure no recurrence in the future. MPSB have confirmed that they did not receive any intercepted product in any of the three cases after the instructions to cease interception were given to the CSPs.

47. HM Customs and Excise (HMCE) reported four errors. The first error occurred when digits in the intercepted telephone number were transposed. Although the application to the Home Office for a warrant contained the correct telephone number the number actually intercepted by the CSP was incorrect by one digit. Checking procedures appear to have failed to spot the error. These have now been tightened.

48. The second error occurred when a new computer system installed in HMCE to manage its warrantry processes mistakenly put a case identifier on a new warrant that had been previously applied to a cancelled warrant. HMCE have been in contact with the company who developed the software for managing their warrantry and has asked them to build a safeguard so that, in future, case identifiers cannot be placed onto cancelled warrants.

49. In the third case, a typing error in the processing of HMCE's documentation resulted in the wrong surname being used on the warrant: a wrong letter was used in the surname. On discovering the error the Home Office was notified and an application was re-submitted in the proper name. No illegal interception took place.

50. The fourth error occurred when HMCE obtained two warrants for two mobile telephone numbers provided by Dutch police who were running a parallel investigation. It transpired that the mobile numbers were incorrect in that an additional digit was included. The additional digit meant that the numbers would not be capable of interception. HM Customs and Excise have assured me that there has been no collateral intrusion in respect of any third parties.

51. The National Criminal Intelligence Service reported one error where a warrant contained an incorrect telephone number: individual digits within the number being transposed incorrectly. Interception ceased immediately the error was discovered: no product was intercepted. NCIS acknowledge that this was clearly a case of simple human error and they will continue to review their procedures to ensure that future recurrences are minimised.

52. No errors were reported by the Ministry of Defence.

53. I now turn to give two examples of the eleven errors made by the communications service providers (CSPs).

54. The first, reported by the Home Office, concerns a CSP who, when testing its new data interception capability, intercepted an e-mail account owned by the National Technical Assistance Centre (NTAC). Whilst this was an acceptable and necessary technical activity agreed with NTAC, part of the equipment failed to function correctly during the test. The consequence of the failure left the account open to access from a non-NTAC user. A detailed technical solution was identified and implemented with the material received by NTAC during the testing having been destroyed.

55. The Scottish Executive reported to me an erroneous termination of an intercept by a CSP. The CSP have acknowledged that the line was cancelled by them in error and that the action resulted in product not being available for a considerable length of time. The CSP has reviewed its systems monitoring procedure and revised their “housekeeping” practices to ensure that a similar situation does not recur. The Scottish Executive also reported a further eight errors by CSPs. The main reasons for these occurring include the wrong technical applications being applied by the CSPs to the intercepting facility, failure to activate a line facility, and the incorrect programming of a number into the computer system.

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 2003, 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 2003

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2003 and (b) issued during the period 1 January 2003 and 31 December 2003

	a	b
Home Secretary	705	1878
The total number of RIPA modifications from 01/01/2003 – 31/12/03 = 2525		
Scottish Executive	41	105
The total number of RIPA modifications from 01/01/2003 – 31/12/03 = 319		

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

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

Order through the Parliamentary Hotline *Lo-call* 0845 702 3474

Fax orders 0870 600 5533

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 0-10-292934-3



9 780102 929348