Report of the Interception of Communications Commissioner for 2004

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
3 November 2005

Laid before the Scottish Parliament
by the Scottish Ministers
November 2005

HC 549
SE/2005/203

£5.50

Report of the Interception of Communications Commissioner for 2004

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
3 November 2005

Laid before the Scottish Parliament
by the Scottish Ministers
November 2005

HC 549
SE/2005/203

Contents

From: The Right Honourable Sir Swinton Thomas

The Interception of Communications Commissioner
c/o 2 Marsham Street
London SW1P 4DF

12 July 2005

Dear Prime Minister,

I enclose my fifth 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the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published.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 2004

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 was re-appointed as the Interception of Communications Commissioner until 10 April 2006. This is my fifth annual report as Commissioner and covers the year ending 31 December 2004.

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. 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. Insofar as it is humanly possible to be, I am satisfied that those responsible are fully conversant with the legislation, and that their practices and procedures comply with it.

4. As I have detailed in previous Reports, my functions as Commissioner are set out in section 57 of the Act and, for ease of reference, are as follows:

- To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 1 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 36 to 38 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 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.

6. Chapter II of Part I came into force on 5 January 2004 (see my report at paragraphs 20-22).

7. Part III (sections 49 to 56, together with Schedule 2) of RIPA is not yet in force. Part III provides for the acquisition of the means to access or decrypt protected electronic data. However, the use of information security and encryption products by terrorist and criminal suspects is not, I understand, as widespread as had been expected when RIPA was approved by Parliament in the year 2000. Equally the Government's investment in the National Technical Assistance Centre – a Home Office managed facility to undertake complex data processing – is enabling law enforcement agencies to understand, as far as necessary, protected electronic data. I understand the Government is keeping under review the need to implement Part III of RIPA and that a public consultation may be held later this year.

8. 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 on some occasions 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 that those concerned with interception fully understand the safeguards and the codes of practice.

9. I continue to be 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.

10. During the year I also met the Home Secretary, the Foreign Secretary, the Secretary of State for Northern Ireland, the Secretary of State for Defence and (in the absence of the First Minister) the Justice 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".

11. During 2004 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 play the important role of executing 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.

12. At the beginning of 2004 I met Sir Stephen Lander and provided him with evidence on the issue of the interception of communications for his review into identifying the right resources and capabilities required for the planned new Serious Organised Crime Agency (SOCA). The Home Secretary announced the formation of SOCA on 9 February 2004.

13. Between 3-5 October 2004 I attended the fourth international biennial conference of the Intelligence Review Agencies in Washington DC, USA. The theme of the conference was "Balancing National Security and Constitutional Principles within a Democracy". I was asked, and gladly agreed, to address the conference on the "Role of the Judiciary in Intelligence and National Security". Members of the Intelligence and Security Committee were also present at, and addressed, the conference. There were delegates from a large number of countries from round the world, and the primary topic for discussion was the oversight, legislative, judicial, or otherwise of intelligence and law enforcement agencies in their intelligence work. I found the discussions during the conference and in the course of informal meetings to be interesting, informative and valuable.

14. In November 2004 I met a team of officials from Hong Kong who had been tasked by the Hong Kong Special Administrative Region Government to examine various issues relating to the interception of communications. The visit focused on how the United Kingdom legislation works in practice, the methods of oversight and accountability, compliance with the Human Rights Act and admissibility of intercepted material as evidence. The discussion I had with the team was wide-ranging and fruitful.

The Extent of Interception: General

15. As in the past, the Annex to this Report contains a summary of the numbers of warrants in force at the end of 2004 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 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. The number of errors reported to me during 2004 is 45, an increase of six on the figure of 39 recorded in my Report last year. I remain of the view that this level of mistakes is still unacceptably high and impress this on the agencies concerned. They accept this and continue to strive to eliminate or at least reduce the number. However it is important to record in this context that with the substantial increase in terrorism and the threat of terrorism, and the increase in serious crime, so the number of warrants and modifications have, of necessity, substantially increased. It is, I think, fair to point out, that if, instead of taking raw numbers, one looks at the number of errors as a percentage of the warrants issued, the percentage of errors has fallen since my previous reports. This is particularly true of the Security Service. It is also important to stress that the number of errors in comparison to the number of warrants is, in percentage terms, very small indeed. This is not to condone them. 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

16. 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.

17. During 2004 I had sight of the revised safeguards documents produced by the National Criminal Intelligence Service and the Metropolitan Police Special Branch. I provided my comments on these documents which fully meet the requirements of section 15 of RIPA.

18. During my visit to Belfast in late 2004 I was shown a copy of the Northern Ireland Office's new safeguards document which had been approved by the Secretary of State for Northern Ireland on 25 October 2004. I have since received a copy of this document, and they also fully comply with the requirements of Section 15 of RIPA.

19. 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 and that the proportionality requirements in the warrants are met effectively in practice. I am satisfied that the agencies are operating effectively within their safeguards.

Communications data

20. 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 by or under Chapter II of Part I. 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). A draft Code of Practice giving guidance on the correct procedures for applying this provision under RIPA is currently subject to public consultation. I provided the Home Office, the department responsible for developing the Code of Practice, with my comments of the content of the draft Code.

21. For better or worse, but inevitably, bringing into force of Chapter II will result in a major change in the role of the Commissioner, and a very large increase in my work and that of the Secretariat. In addition to the agencies covered by Chapter I of Part I of RIPA, and the prisons (138 in number) there are 52 police forces in England, Wales, Scotland and Northern Ireland and 510 public authorities who are authorised to obtain communications data, all of whom will have to be inspected. This is clearly a major task which could not be carried out by one person. Hence the need for a Chief Inspector and Inspectors.

22. I mentioned in paragraph 20 of my Report last year that I had numerous meetings with officials at the Home Office with the aim of establishing the appropriate oversight regime and the level of resources required. A recruitment campaign was initiated in August 2004 to identify and appoint a Chief Inspector and an appropriate number of Inspectors to help me in my oversight of Chapter II as well as my non-statutory role of overseeing interception in prisons. Suitable candidates have been identified. They should be in post before the summer, although they will have to be trained before they undertake inspections. I will continue to keep the oversight of the interception of communications under Chapter I within my sole remit.

23. Although no formal oversight regime was in place during 2004 work was, and continues to be, undertaken to gather statistical information from all the empowered police and public authorities on their use of the powers conferred on them under RIPA Part I Chapter II, specifically (i) the number of requests made for subscriber details, (ii) the number of requests made for details of incoming and outgoing data, (iii) details of any other types of data, and (iv) the total number of errors that occurred during the application process. I intend providing these details, and a report of the oversight inspections undertaken during 2005, in my 2005 Annual Report.

Section 17: Exclusion of matters from legal proceedings

24. The question of the admission of intercept material in criminal proceedings has been discussed at some length in the course of 2004 between myself and Ministers, the Security and Intelligence Co-ordinator, the security, intelligence and law enforcement agencies and the communication service providers. The aim of all concerned is, of course, to use this material to the best advantage to prevent terrorism and crime, and to apprehend terrorists and criminals. The subject is a complex one, much more complex than at first sight might appear. It is not suitable for lengthy discussion in this Report. I have the considerable advantage in my position of having an overall picture of all those engaged in this work. I am left in no doubt that the balance falls firmly against any change in the present law and that any amendment of Section 17 of the Act would, overall, be damaging to the work of the security, intelligence and law enforcement agencies. I continue, of course, to have an open mind on this subject if any major change should occur in the future.

Prisons

25. 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 and in paragraph 21 of my 2003 Report I detailed the next four establishments I visited together with one re-visit. During 2004 I visited HM Prison Full Sutton, HM Prison Wandsworth and HM Prison Maidstone.

26. For my visits 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.

27. 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.

28. After each visit I produced an 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.

29. As I mentioned in paragraph 21 above, Inspectors have now been recruited to undertake future inspection visits on my behalf. I will, of course, retain overall responsibility for the conduct of these inspections and any follow-up action that will be required.

Transfer of interception warrants between police forces

30. I was approached by an officer in a Scottish police force (force A) seeking my view on the propriety of "transferring" to his force an interception warrant obtained by, and held by, another Scottish police force (force B).

31. Force B obtained, through the Scottish Executive, an interception warrant signed by the First Minister in Scotland for a target in their force area. The target subsequently moved away from that address to reside in force A's area. Force A questioned whether force B should cancel the existing warrant thus requiring force A to seek a fresh warrant for themselves or can responsibility for the interception work merely be "transferred" between the forces with the existing warrant left in place.

32. I understand the Scottish Executive was approached about this matter who confirmed that, as far as they can establish, there is no precedent in Scotland for "transferring" a warrant. My advice was that under section 5 of RIPA a fresh warrant would be required – the existing one for force B being cancelled and a new one obtained addressed to the Chief Constable of force A.

Foreign and Commonwealth Office and Northern Ireland Office warrants

33. 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.

34. 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."*

35. 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

36. The Investigatory Powers Tribunal (the Tribunal) was established by section 65 of RIPA. 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 for 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, one of whom, I am sad to report, died in the summer of 2004. A Registrar has also been appointed to help in the process of hearing claims alleging infringements of the Human Rights Act.

37. As I explained in paragraph 25 of my Annual Report for 2000, complaints to the Tribunal cannot easily be "categorised" under the three Tribunal systems that existed prior to RIPA. Consequently, I am unable to detail those complaints that relate to the interception of communications that would have previously been considered by the Interception of Communications Tribunal. I can only provide the information on the total number of complaints made to the Investigatory Powers Tribunal. The Tribunal received 90 new applications during 2004 and completed its investigation of 49 of these during the year as well as concluding

its investigation of 66 of the 76 cases carried over from 2003. 51 cases have been carried forward to 2005. On no occasion during 2004 has the Tribunal concluded that there has been a contravention of RIPA or the Human Rights Act 1998.

Assistance to the Investigatory Powers Tribunal

38. 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 2004.

Rulings on Preliminary Issues of Law

39. The Investigatory Powers Tribunal have handed down two important and related Rulings on Preliminary Issues of Law on 23 January 2003 and 09 December 2004. The judgments cover a number of issues which it is not appropriate for me to set out in this Report, but, for those who are interested, they can be accessed shortly on the Tribunal's website [www.ipt-uk.com].

40. The Ruling of 23 January 2003 does not directly affect my role as Commissioner, but the Ruling of 09 December 2004 does have relevance to it, and I will, therefore, quote the relevant passages:

Paragraph 3:

> The issue was whether, as formulated by the Complainants' Counsel, *"the process of filtering intercepted telephone calls made from the UK to overseas telephones … breaches Article 8(2) [of the European Convention on Human Rights] because it is not "in accordance with the law"*. Article 8 reads as follows:
>
> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. 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, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Paragraph 5:

> RIPA provides for two different "regimes": the s81(1) regime with regard to the interception of communications transmitted and received within the United Kingdom ("internal telecommunications") and the s8(4) regime, relating to telephone communications between the United Kingdom and abroad ("external communications"). However, there are, as will be seen, substantial similarities between the provisions governing such regimes. In particular, both the s8(1) and s8(4) warrants are subject to the provisions of s5 of RIPA, which provides for the issue of warrants in relation to the interception of communications by the Secretary of State in subsection (1).

Paragraph 6:

> The relevant provisions governing both regimes are contained in the following subsections of s5:
>
> *"(2) The Secretary of State shall not issue an interception warrant unless he believes –*
>
> *(a) that the warrant is necessary on grounds falling within subsection (3); and*

(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary –

(a) in the interests of national security;

(b) for the purpose of preventing or detecting 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.

(3) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means…

41. At paragraph 14 the Tribunal made reference to a statement made by the Director General of the Organised Crime, Drugs and International Group of the Home Office, and then at paragraph 33 referred to paragraph 14 of that statement which said

"…This process under section 8(4) permits selection and examination of the selected material only to the extent that to do so would be necessary in the interests of national security, to prevent or detect serious crime or to safeguard the economic well-being of the United Kingdom. In this regard and generally, section 8(4) is to be read in conjunction with section 15 of [RIPA], which in subsection (1)(b) specifically makes section 8(4) warrants subject to arrangements for ensuring that the requirements of section 16 of [RIPA] are satisfied (namely "that intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c)"). It is the duty of the Secretary of State to ensure that such arrangements are in force that he considers necessary for securing that the requirements of s16 are satisfied."

The Tribunal then continued:

Paragraph 39:

The provisions, in this case the right to intercept and access material covered by a s8(4)warrant, and the criteria by reference to which it is exercised, are in our judgment sufficiently accessible and foreseeable to be *in accordance with law*. The parameters in which the discretion to conduct interception is carried on, by reference to s5(3) and subject to the safeguards referred to, are plain from the face of the statute. In this difficult and perilous area of national security, taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed upon the Respondent, we are satisfied that the balance is properly struck.

Errors

42. The following should be read in the context of my general comments in paragraph 15 of this Report. A significant number of errors and breaches have been reported to me during the course of the year – 45 in all. This reflects an

increase of 6 on the 39 errors reported in 2003. The number of errors is 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.

43. Two incidents occurred in the **Home Office** which were duly reported. The first concerned their failure to issue a ratification for a modification made under the emergency procedures. A period of unauthorised interception ensued until the administrative error was spotted and a new schedule issued. The second related to the misplacement within the Home Office of a sensitive letter. An investigation has been launched to establish the circumstances of this incident.

44. The **Scottish Executive** reported one error where a warrant contained an incorrect telephone number: individual digits within the number being transposed incorrectly. The error was made by the relevant police force and not by the staff of the Scottish Executive.

45. The **Northern Ireland Office** reported six errors. In one case a warrant was properly obtained against the target but product revealed that the telephone numbers quoted on the warrant were incorrect and that the telephone was not, in fact, used by the intended target. All product was destroyed.

46. In another case an error occurred when a warrant was obtained quoting the correct telephone number and the name of the target which intelligence revealed was the wrong person. The warrant was cancelled and a new one against the correct target name was obtained.

47. Two further errors were reported where warrants contained incorrect telephone numbers: individual digits within the numbers being transposed incorrectly.

48. In two other cases a digit was included in the warranted telephone number which is normally omitted from the prefix. Unfortunately the technology, having recognised that the number was one figure longer than acceptable, omitted the last digit of the number resulting in the interception of unidentified people unrelated to the targets. The warrants were cancelled and all product destroyed.

49. Eight errors were reported by **GCHQ** of which four are briefly highlighted below. The first case concerns the inclusion of a selector in a targeting database even though no modification had been signed to add the selector to a schedule of an existing warrant. Following discovery of the error two weeks later the selector was removed from the database. New procedures have been put in place within the relevant areas of GCHQ to prevent a recurrence of a similar error.

50. The second error arose out of avoidable human error. Instructions to cease collection were only issued to three of the four communication service providers served with schedules under an existing warrant. The relevant GCHQ officer left a message with the fourth communication service provider but he failed to make it clear on the check sheet used for these purposes that a reply was still pending. Twelve days elapsed after the modification of schedules before it became clear that collection by the fourth provider had not ceased. The relevant staff have been reminded of their responsibilities in ensuring the correct procedures are followed in future.

51. The third case also arose out of avoidable human error. A target whose calls

were being intercepted under GCHQ's RIPA 8(4) warrants travelled to the United Kingdom for a weekend. GCHQ had concluded that interception during this period would be of no intelligence value and so did not obtain the appropriate RIPA authorisation to continue targeting. Because of an incorrect entry in a database, targeting resumed the day before the person left the UK. Four calls were selected for listening but were then destroyed.

52. The fourth error arose out of feasibility checking for a selector prior to adding it to a warrant issued under section 8(1) of RIPA. During the check the GCHQ analyst found an existing entry for the selector under a specific warrant. Unfortunately he failed to notice that the latter was not a RIPA interception warrant and went on to add the selector to a targeting database. The position was rectified immediately upon discovery. Although 86 items were selected no reports were issued. The error was as a result of human error. Tasking procedures have been revised to ensure no recurrence of similar errors.

53. The **Security Service** reported sixteen errors, brief details of six of these are highlighted below. In the first case, warrants against a target's landline and mobile telephones were cancelled but it transpired that the interception of traffic on the landline had not been stopped. No product was received. The Service has re-examined its procedures for handling and monitoring interceptions to prevent similar recurrences.

54. The second error occurred in respect of a modification. A modification was made to an existing warrant with the modification document itself correctly recording the telephone number. A copy of the modification was forwarded to the Home Office. However, the formal application to the Home Office to ratify the modification, which the Home Office processed and duly provided a signed modification instrument, contained an error in that digits were incorrectly transposed. The error was, unfortunately, missed by both the Security Service and the Home Office.

55. In the third case, the Security Service reported that they had confused two telephone numbers relevant to an investigation resulting in an intercept warrant being obtained for an associate of the target rather than the target himself. The intercept was suspended and the correct telephone number added to the warrant. No communications were listened to or transcribed and the product was destroyed.

56. A fourth error occurred when, due to an inputting error on their warrantry records database, the Security Service failed to request the cancellation of a warrant. No interception took place after the warrant expired and, unfortunately, neither the Home Office nor the communication service provider noticed that the warrant had not been renewed or cancelled.

57. Errors were reported in two separate cases when target telephone numbers had been mis-transcribed and the numbers placed on interception were incorrect. The errors were not apparent to the four UK mobile network providers on whom schedules were served. The interceptions were suspended and the incorrect numbers deleted. No product was received in either case.

58. The **Secret Intelligence Service (SIS)** reported an error in that they failed to report to me, as required by the Code of Practice for the interception of communications, the fact that some information that was considered to be subject to legal privilege had been transcribed under a warrant. In light of this error SIS have amended its administrative processes for the handling of confidential information whether on legal, religious, journalistic or medical grounds.

59. **HM Revenue and Customs (HMRC)** reported one error. The error occurred when HMRC failed to request a cancellation of a warrant and only did so after the warrant had expired. HMRC has reviewed its internal systems and has taken steps to prevent a recurrence. No product was received after the decision

was taken to cancel the warrant. The delay was in making the formal cancellation request.

60. The **National Criminal Intelligence Service (NCIS)** reported one error where an NCS warrant contained an incorrect telephone number: an incorrect digit had been included in the application. Interception ceased immediately the error was discovered. This error has identified areas where the application process within the NCS and NCIS can be improved and steps have been put in place to prevent future recurrences.

61. No errors were reported by the Metropolitan Police Special Branch or the Ministry of Defence.

62. I now turn to give two examples of the ten errors made by the **communications service providers (CSPs)**.

63. The first, reported by the Security Service, concerns a feasibility check they requested of a CSP for a mobile telephone number. The Security Service requested a response by 11am on a particular day but, unfortunately, the relevant CSP mistakenly thought that the warrant itself was going to be signed by 11 am and rather than wait for the confirmatory telephone call from the warrant-issuing department the CSP started the interception at 1045 am. On discovering the error the interception was suspended.

64. The second error, reported by the Scottish Executive, occurred when a CSP had a wrong case identification number logged against an intercept resulting in a loss of product for six days. The case identification number was different to that allocated when the schedule to the interception warrant was served on the CSP.

Conclusion

65. As I highlighted in my Report last year, the interception of communications is an invaluable weapon for the purposes 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.

66. It is my view that in 2004, 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 continue to carry out this task diligently and in accordance with the law.

Annex to the report of the Commissioner for 2004

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2004 and (b) issued during the period 1 January 2004 and 31 December 2004

	a	b
Home Secretary	674	1849
The total number of RIPA modifications from 01/01/2004 – 31/12/2004 = 3101		
Scottish Executive	34	124
The total number of RIPA modifications from 01/01/2004 – 31/12/2004 = 266		

[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 by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 182601 10/05 317035 19585

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

Online
www.tsoshop.co.uk

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 7 023474
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 0-10-293564-5

9 780102 935646