Report of the Interception of Communications Commissioner for 2006

Commissioner:
THE RT HON SIR PAUL KENNEDY

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
28 January 2008

Laid before the Scottish Parliament by
the Scottish Ministers
January 2008

HC 252
SG/2008/9

Contents

From: The Right Honourable Sir Paul Kennedy

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

24 October 2007

I enclose my first Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. The Report covers my first nine months in office from 11 April 2006 to 31 December 2006. 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, or 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 predecessors, 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the course of writing the report in two parts, the Confidential Annex containing those matters which in my view should not be published.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 Paul Kennedy

The Rt. Hon. Gordon Brown MP
10 Downing Street
London SW1A 2AA

Annual Report of the Interception of Communications Commissioner for 2006

Introduction

1. On 11 April 2006 I was appointed the Interception of Communications Commissioner under Section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA) in succession to the Right Honourable Sir Swinton Thomas. My appointment is for a period of three years. From that date until 31 July 2006 Sir Swinton Thomas supported me on a complete round of inspections of all the Agencies set out in section 6(2) of RIPA, and all the major Communication Service Providers (CSPs) engaged in this work, as well as a number of meetings with representatives of the Agencies to deal with issues that have arisen since my appointment. I am grateful to Sir Swinton Thomas for his assistance and invaluable advice during this period.

2. I am required by section 58(4) of RIPA as soon as practicable after the end of each calendar year to report with respect to the carrying out of my functions as the Interception of Communications Commissioner. This is my first annual report as Commissioner and it covers my first nine months in office: 1 April 2006 until 31 December 2006. In producing my report, I propose to follow, as my predecessors have done, the practice of writing the report in two parts, this main part for publication, the other part being a confidential annex to include those matters which cannot be fully explained without disclosing sensitive information.

Functions of the Commissioner

3. I was appointed under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). The coming into force of 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.

4. As Commissioner I have three main functions: these are set out in section 57 of RIPA 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.

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. Part III (sections 49 to 56, together with Schedule 2) of RIPA – which provides for the disclosure of protected electronic data in an intelligible form or for disclosure of the means to access to such data to make it intelligible – will enter into force on 1st October 2007.

Part I Chapter I: Interception

7. I have decided to continue with the practice followed by my predecessors of making twice yearly visits to the Security Service, the Secret Intelligence Service, Government Communications Headquarters, the Serious Organised Crime Agency, the Metropolitan Police Counter Terrorism Command, Strathclyde Police (visited once in this reporting period), the Police Service for Northern Ireland, the Northern Ireland Office, HM Revenue and Customs, the Foreign and Commonwealth Office, the Home Office, the Scottish Executive (visited once in this reporting period), and the Ministry of Defence. In short, I meet officers in the agencies undertaking interception work and officials in the departments of the Secretaries of State/Ministers which issue the warrants. Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since the previous visit of either myself or Sir Swinton Thomas. I then select, largely at random, a sample of warrants for inspection. In the course of my visit I satisfy myself that those warrants fully meet the criteria 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 with the officers concerned. I can, if I need to, view the product of interception. It is of paramount importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

8. I have been impressed by the quality, dedication and enthusiasm of the personnel carrying out this work. They possess a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards. All applications made to the Secretary of State are scrutinised by officials in the warrants unit within their respective Departments (e.g., the Home Office, the Foreign Office and the Ministry of Defence and by similar officers in departments in the Northern Ireland Office and Scottish Executive). They are all skilled in their work and there is very little danger of any defective application being placed before the Secretary of State. I will refer in some detail to errors which have occurred during the period under review. Where errors have occurred, they are errors of detail or procedure and not of substance. The Agencies always make available to me personnel and documents that I have requested. They welcome my oversight as ensuring that they are acting lawfully and appropriately and seeking my advice 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 left in no doubt at all as to the Agencies' commitment to comply with the law. In case of doubt or difficulty, they do not hesitate to contact me and to seek advice.

9. During the first nine months of my appointment I have not had the opportunity of meeting the Home Secretary, the Foreign Secretary, the Secretary

of State for Defence, the Secretary of State for Northern Ireland or the First Minister for Scotland. I did, however, meet the Justice Minister for Scotland. It was evident from my discussion with her that she gives a substantial amount of time and considerable care to satisfy herself that warrants are necessary for the authorised purposes, and that what is proposed is proportionate. If she wanted further information in order to be satisfied that she should grant the warrant then it is requested and given. The Justice Minister confirmed that outright refusal of an application is comparatively rare, because the requesting police forces and the senior officials in her Department scrutinise the applications with care before they are submitted for her approval. However, she may refuse to grant the warrant if she considers, for example, that the strict requirements of necessity or proportionality are not met.

10. Since my appointment, I have visited eleven communication and internet service providers (CSPs) consisting of the Post Office and the communications companies who are most engaged in interception work. These visits, mostly outside London, are not formal inspections but are designed to enable me to meet both senior staff in each company as well as the personnel who carry out the work on the ground, and for them to meet and talk to me. I have no doubt that the CSPs and their staff welcome these visits. We discussed the work that they do, the safeguards that are in place, any errors that have occurred, any legal or other issues which are of concern to them, and their relationships with the interception agencies. Those in the CSPs who work in this field have great enthusiasm in their work. They recognise the importance of it in the public interest, and the necessity of doing all their work accurately and efficiently, and show considerable dedication to it.

11. Between 2 – 4 October 2006 I attended the fifth international biennial conference of the International Intelligence Review Agencies in Cape Town, South Africa. The theme of the Conference was "Balancing National Security and Constitutional Principles within a Democracy". Members of the Intelligence and Security Committee were also present. There were delegates from a large number of countries from around the world – including Australia, Belgium, Canada, the Netherlands, New Zealand, Norway, Poland, South Africa and the United States of America – 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.

Part I Chapter II: Acquisition and disclosure of communications data

12. On 5 January 2004 Chapter II of Part I of RIPA came into force enabling named public authorities approved by Parliament to acquire and disclose communications data. Although an important and an extremely powerful and effective investigative tool, the acquisition and disclosure of communications data is not as intrusive as the interception of communications themselves. Currently, the number of public authorities that I am required to inspect and oversee under Part I Chapter II of RIPA are as follows:

a. The security and intelligence and law enforcement Agencies – the Security Service, Secret Intelligence Service and Government Communications Headquarters.

b. The Serious Organised Crime Agency and HM Revenue and Customs.

c. 52 police forces.

d. 12 other Law Enforcement Agencies such as the Royal Military Police and the British Transport Police.

e. 474 local authorities authorised to acquire communications data.

f. 110 other public authorities such as the Financial Services Authority, the

Serious Fraud Office, the Independent Police Complaints Commission, the Ambulance Service and Fire Authorities who are authorised to acquire communications data.

13. As Sir Swinton Thomas highlighted in his final Annual Report, it would be impossible for a single Commissioner to inspect and report on all these organisations on his own. Some inspections are quite lengthy, occasionally running to several days, and full Reports have to be prepared for each authority inspected. Accordingly a Chief Inspector and a team of five Inspectors were recruited to carry out the bulk of the inspections under Part I Chapter II of RIPA in respect of the acquisition and disclosure of communications data. I retain personal responsibility for all oversight under Part I Chapter I (Interception of Communications).

Communications Data and the Work of the Inspectorate during this Report period

14. The acquisition of communications data is a very valuable investigative tool, and is primarily aimed at acquiring information in relevant cases as to "who", "when" and "where". It is valuable in terrorist and criminal cases, for example kidnapping cases, and tracing missing persons and identifying seriously injured people and attempted suicides (e.g., by the Ambulance Service and the Maritime and Coastguard Agency).

15. Those public authorities entitled to acquire communications data are set out in Section 25 of Chapter II of Part I of RIPA and subsidiary legislation and have been approved by Parliament. The Act defines communications data and in Section 22 sets out the requirements and conditions that must be fulfilled before communications data can be acquired. In particular, it must be shown that it is necessary to acquire the data as defined in the section (e.g., for the purpose of preventing or detecting crime or preventing death or injury) and is proportionate to what is sought to be achieved by obtaining the data.

16. The objectives of the Inspectors are to ensure that communications data is being acquired in accordance with the Act and the draft Code of Practice, and in particular to ensure that the principles of necessity and proportionality are being complied with, and to ensure that relevant records are kept, that errors are reported, and that training for those involved in this area of work is adequate. In this way independent oversight is provided and good and bad practice is identified and fed back into the inspection process.

17. Since they commenced their inspections in the autumn of 2005, the Chief Inspector and the Inspectors have undertaken a significant visits programme:

- 101 prisons visited
- 19 prisons revisited
- 37 local authorities visited
- 6 local authorities revisited
- 52 police forces visited
- 2 police forces revisited
- 3 intelligence agencies visited
- 12 law enforcement agencies visited
- 12 miscellaneous public authorities visited

It was necessary for the Inspectors to conduct early re-inspections of a few of the public authorities because some weaknesses were found in parts of their system and processes, which did not mean that they were acting unlawfully but they did make it difficult for them to achieve the best possible level of compliance with the Act and Code of Practice. Without exception these weaknesses were quickly remedied and the systems were made fit for purpose. In the future re-visits will be made to ensure that standards are maintained.

18. Not all local authorities make use of their powers, some only making minimal use or not using them at all. I will return to this later. Each inspection may take anything from one to four days. Most can be completed in one or two days and I anticipate that once all the first inspections have taken place then future inspections should not take more than one or at the most two days. After each inspection a Report is written and recommendations made.

Inspections of Police Forces

19. The Police Forces who had, before the introduction of RIPA, obtained communications data primarily through the communications service providers making disclosures under the Data Protection Act, have acclimatised themselves to the new procedures. They are now required to comply not only with the legislation, but also with the draft Code of Practice which has been prepared by the Home Office in collaboration with the Association of Chief Police Officers (ACPO), and representatives of the local authorities and the communications service providers (CSPs). The draft Code of Practice has been through several drafts and much consultation, and has now been approved by Parliament and will come into force from 1st October 2007. In the initial stages there were some complaints that the legislation and/or its processes were over-bureaucratic, and difficult to manage. It is quite complex, but not difficult and it is designed to ensure that all acquisition and disclosure of communications data is carried out lawfully and that the rights of the citizen are properly protected. Police Forces have acclimatised themselves to the legislation and the draft Code of Practice, and now find that they are quite simple to comply with.

20. Reflecting what appears in paragraph 16 above, the primary objectives of the inspection of Police Forces are to:

(a) ensure that the systems in place for acquiring and utilising communications data are sufficient for the purposes of the Act, and that all relevant records have been kept for inspection;

(b) ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act, Chapter II of Part I of RIPA and the draft Code of Practice;

(c) provide independent oversight of the process and ensure that the data which has been obtained was necessary and proportionate to the conduct being undertaken;

(d) ensure that errors are being reported and that the systems are reviewed and adapted in the light of any exposed weaknesses or faults;

(e) identify good and bad practice, and disseminate the findings after consultation with the Home Office;

(f) ensure that persons engaged in the acquisition and disclosure of data are adequately trained and are aware of the relevant parts of the legislation.

21. The Inspectors found on the whole that the standard applied was good. Inevitably there were some failings. Full reports were prepared, together with Action Plans with recommendations. These Reports are forwarded to the relevant Chief Constable. In every instance, the Reports have been welcomed and the Action Plans and recommendations have been accepted.

Acquisition of data by Local Authorities and other Public Authorities

22. As indicated in paragraph 12 above, 474 Local Authorities are empowered to obtain communications data, of whom only 122 made use of their powers to acquire communications data during the period covered by this Report. A total of 1,694 requests were made for communications data by these Local Authorities

during the same period and the vast majority of these were for subscriber information under Section 21 (4)(c) of RIPA. Local Authorities are restricted to acquiring communications data for the purpose of preventing and detecting crime and mostly this involves the investigation of offences by the Trading Standards Service, Environmental Control and Housing Benefits Departments. Invariably communications data is only applied for as a last resort and to identify suspected criminals, including rogue traders, fly tippers and fraudsters. Since the inspection regime was formed in May 2005 my Inspectors have visited 44 Local Authorities and they have been satisfied that they have been acquiring communications data lawfully and for the correct purpose. Naturally the Inspectors have been concentrating upon the Local Authorities which have made the most use of their powers and the remainder, which have still to be visited, have generally made only a handful of requests.

23. During the period covered by my Report only six of the Fire Services used their powers to acquire communications data and they generated a few requests for subscriber information. Of the 110 other public authorities, only 32 are using their powers. I am a little concerned that there continues to be a number of authorities who applied for the powers to be given to them and who apparently do not use them and I do not know why this is so. It may be that they have not as yet set up appropriate mechanisms to obtain communications data, but if this state of affairs continues unexplained, then consideration must be given to removing the powers from them.

24. Inspections have taken place of all those authorities that are making significant use of their powers. Inevitably, the results have been variable. On the whole, however, the Inspectors have been impressed by the systems in place and by the fact that the applications are being made in accordance with the law and the draft Code of Practice. The objectives of the inspections are broadly similar to those with police forces.

25. Following the inspections, full Reports together with Action Plans have been sent to the Local or Public Authority concerned. They have been welcomed, and the recommendations accepted.

Interception in Prisons

26. I have, at the request of the Home Secretary, continued in a non-statutory role, the oversight of the interception of communications in prisons, which was undertaken by my predecessor. Interception of communications (mail and telephone communications) in prisons is permitted, and in many cases is mandatory, under the Prison Act 1952, and the National Security Framework (NSF). Interception is mandatory primarily in the case of Category A prisoners, and prisoners who have been convicted of sexual or harassment offences, and continue to present a risk to the public. So far as Category A prisoners are concerned, this presents a problem in many prisons, because they do not have the resources to monitor all the telephone communications. The same can apply to those convicted of sexual or harassment offences, particularly if they are gathered together in one prison.

27. Interception is illegal and a breach of the Human Rights Act unless it is carried out in accordance with the Act and the NSF.

28. There are three primary areas of inspection:

- the methods utilised for the interception of telephone and postal communications to ensure that the interception is being carried out lawfully;
- 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.

29. Compliance with these requirements varied from prison to prison but it is fair to say that since the introduction of the inspection regime, the Prison Service has made strenuous efforts to ensure that there is compliance. Again, at the conclusion of each inspection, a Report and an Action Plan has been sent to the Governor of the prison concerned. These have been accepted, and subsequent inspections have usually shown considerable improvement. I am reasonably confident that in time inspections will show that there is general compliance with the Act and with the Rules laid down under the Act. It is of the first importance that this should be achieved and that inconsistencies in performance are eliminated.

30. Since my predecessor began to inspect prisons he and I, using an excellent team of Inspectors who have worked under our Chief Inspector, have been responsible for visits to a total of 132 prisons. 31 have now been re-visited. Re-visits are arranged more quickly if it is considered necessary to check that improvements have been made, but in general the object of re-visiting is to ensure that standards are maintained.

Foreign and Commonwealth Office and Northern Ireland Office Warrants

31. 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.

32. 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."

33. 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.

Serious Organised Crime Agency (SOCA)

34. The Serious Organised Crime Agency (SOCA) was established on 1 April 2006 and was formed from the amalgamation of the National Crime Squad (NCS), National Criminal Intelligence Service (NCIS), that part of HM Revenue

& Customs (HMRC) dealing with drug trafficking and associated criminal finance and a part of UK Immigration dealing with organised immigration crime (UKIS).

35. SOCA is an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is the damage caused to people and communities by serious organised crime. The Agency will focus on, and target, those criminals involved in drugs, human trafficking, major fraud and counterfeiting. The use of interception warrants will be an important weapon in the Agency's fight against such serious crime.

HM Revenue & Customs (HMRC)

36. With the establishment of the Serious Organised Crime Agency (SOCA) on 1 April 2006, organisational changes took place within HM Revenue & Customs (HMRC). From that date HMRC no longer has prime responsibility for the investigation of large scale drugs smuggling, which previously formed a substantial part of its work. Nevertheless, the level of criminality involved in the fiscal frauds that remain within HMRC's investigation remit is high with interception being an effective tool in the investigation of non-commodity based fraud.

37. During the period of this report, HMRC considered whether the statutory denial of the use of interception (and other powers) in the investigation of former Inland Revenue matters (within the Commissioners of Revenue and Customs Act 2005) was still appropriate in the light of evidence that serious organised crime groups have become active in that area. HMRC believes that where the threshold of serious crime is crossed, and it is necessary and proportionate to do so, it is appropriate to use interception, and I understand provision has been made within the current Serious Crime Bill to remove the existing statutory restrictions.

The Investigatory Powers Tribunal

38. 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, five 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.

39. As my predecessor, Sir Swinton Thomas, explained in paragraph 25 of his 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 86 new applications during the calendar year 1 January 2006 – 31 December 2006 and completed its investigation of 43 of these during the year as well as concluding its investigation of 38 of the 52 cases carried over from 2005. 57 cases have been carried forward to 2007.

Assistance to the Investigatory Powers Tribunal

40. 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 2006.

Safeguards

41. 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, disclosing, 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 is sought on proposed amendments to the safeguards when they are updated in light of technical and administrative developments. During the period of this report I saw and commented on the revised handling arrangements for the Scottish Police Service and the safeguards for the new Serious Organised Crime Agency.

Errors

RIPA Part I Chapter I: Interception

42. Twenty-four interception errors and breaches have been reported to me during the course of the 9 month period of this report. This reflects a significant decrease in the errors reported by my predecessor. That said I still consider the number of errors to be too high. By way of example, details of some of these errors 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 error 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., 1965 instead of 1956. The examples that I give are typical of the totality and are anonymous so far as the targets are concerned. Full details of all the errors and breaches are set out in the Confidential Annex.

43. The **Northern Ireland Office/Police Service Northern Ireland** reported seven errors of which five are highlighted below. In two separate cases, warrants were properly obtained against their respective targets but product revealed that the telephone numbers quoted on the warrants were incorrect and that the telephones were not, in fact, used by the intended targets. All product was destroyed.

44. In three other separate cases, the telephone numbers on their respective warrants contained incorrect digits. In one of the cases, no product was obtained: in the other two the product was destroyed. In all cases, the correct numbers were added to their respective warrants.

45. Six errors were reported to me by **GCHQ** of which three are highlighted below. The first case occurred in relation to a request made of GCHQ. A target whose communications were being intercepted because he was expected to have travelled overseas was found to have remained in the United Kingdom, the individual having not travelled as expected. The target's change of plans was reported to GCHQ who failed to take any action upon the information received. No items were intercepted. All personnel have been reminded of the need for care and vigilance in following through information received.

46. The second error occurred in relation to a request made of GCHQ to intercept the communications of four individuals whilst they were overseas. The targets travelled overseas and their expected date of return was reported to GCHQ who were expected to cease targeting on that day. Unfortunately, it was not terminated until the day after their return. Only one item was intercepted but not transcribed or reported. All analysts have been reminded of the correct procedures to follow when a target is found to be in the UK.

47. In the third, and separate, case, four telephone numbers were added to GCHQ's databases to intercept the communications of a target who was known to be overseas. One number was subsequently removed and another was removed when analysts learned that he had re-entered the UK. However, analysts failed to

remove the remaining two telephone numbers which remained targeted for a further three months. Five calls were intercepted during this period though none were listened to and all have been deleted from GCHQ's systems. GCHQ have revised their procedures to help prevent a recurrence.

48. The **Security Service** reported four errors. Brief details of two of these are highlighted below. The first case relates to an intercept of an email address. When a warrant against a target was cancelled one of the email addresses was omitted. The error was an oversight on the part of a desk officer. Security Service officers have been reminded of the importance of keeping accurate records and of carrying out thorough checks of the telephone numbers and addresses listed on the interception warrants prior to their cancellation.

49. In another error, the Security Service processed a modification to add a new mobile telephone number to an existing warrant. Unfortunately the submission with the new telephone number included an incorrect case identifier. The case identifier quoted had previously been allocated to a different mobile number of a different target. This resulted in the wrong telephone number being intercepted. No product was obtained and there was no interference with privacy. Security Service officers have been reminded of the importance of carrying out thorough checks of telephone numbers added to interception warrants.

50. **HM Revenue and Customs (HMRC)** reported two errors, one of which I have highlighted. HMRC made an application for a modification to the schedule to add another telephone number for a warranted target; the modification was authorised and interception commenced. However, concern was expressed about the lack of product. A check revealed that HMRC's application showed an incorrect digit in the telephone number. Interception ceased immediately: as already mentioned no product was received. HMRC has amended its system to strengthen the independent accuracy checks.

51. The **Serious Organised Crime Agency** reported one error where the warrant number for a renewal was incorrectly quoted in a submission to the Home Office. Consequently interception continued on the wrong warrant number. A month later a modification on the correct warrant number for the addition of a telephone number was submitted. A check of all the warrantry paperwork identified the error and the facilities were immediately suspended. I understand a new IT system at SOCA will prevent a recurrence of such an error and that all staff working in the Home Office have been reminded of the importance of keeping accurate records and of carrying out thorough checks.

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

53. The first error, reported by the Police Service of Northern Ireland, occurred when a warrant was cancelled and the CSP was notified but continued to provide product to a sharing agency for a further six weeks. This was as a result of an administrative error at the CSP.

54. The second error, reported by an internet service provider (ISP) themselves, occurred in respect of two warrants that the ISP was instructed to set up by the Home Office. Unfortunately due to a misunderstanding at the ISP, the results of these two warrants were delivered to the wrong agency. Discussions between the ISP and the Home Office have addressed the misunderstanding and no such future error should recur.

55. No errors were reported by the **Home Office, Scottish Executive, Ministry of Defence, Secret Intelligence Service and Metropolitan Police Special Branch**.

RIPA Part I Chapter II: Acquisition and disclosure of communications data

56. All Public Authorities have a duty to report any errors which occur when they are acquiring communications data under Section 5 of the draft Code of Practice. They are obliged to provide an explanation for the errors and most

importantly they must also describe the action which they have taken to prevent similar errors occurring again. The most common types of errors are the transposition of numbers or where numbers have been provided by members of the public and either reported or noted down incorrectly. These are human errors which unintentionally can result in the acquisition of data which is not relevant to the matter under investigation. In such circumstances the Public Authority must destroy the data as soon as it has made its report to my office.

57. Public Authorities also have a responsibility to report any errors which are made by Communications Service Providers (CSPs) in the course of acquiring and disclosing communications data. Generally such errors occur when the CSP concerned discloses data which is in excess of that originally requested by the Public Authority. Often this occurs as a result of a fault in the system or it may be due to a mistake which has been made by the CSP when keying the request into a computer.

58. During the period covered by this report 1,088 errors were reported to my office. A total of 301 of these errors were attributable to CSPs and the remainder (787) were blameworthy errors made by Public Authorities. This may seem a large number but indeed it is very small when compared to the overall number of requests for communications data which totalled 253,557 during the same period. The number of errors equates to approximately 0.4% of the total number of requests. In paragraph 82 of his final report for 2005/2006 my predecessor, Sir Swinton Thomas, concluded that no useful purpose would be served in giving further details about the individual errors. I agree with this stance for the same two reasons that Sir Swinton gave. First the inspections are still ongoing so that any description might well be incomplete and paint a false picture. Second, I am not at present convinced that a useful purpose would be served by a detailed description of the errors in relation to communications data in a report of this nature. I should add that neither I nor any member of my team have found any instances of wilful or reckless conduct and that is why there is no mention of this in the report.

59. My Inspectors work closely with the public authorities and CSPs to review their systems and processes so that errors are kept to an absolute minimum but of course human error can never be eliminated completely. A large number of the law enforcement agencies, who are the principal users of communications data, have acquired fully automated systems and these greatly reduce the scope for keying errors. My Inspectors review all the errors during their inspections and check that the public authorities destroy any data which has been illegally obtained, or which should only be retained for a finite period. Errors which are caused as a result of a breach of the draft Code of Practice by public authorities are fully investigated and the Inspectors ensure that appropriate action is taken to remedy any faults.

60. From the ever increasing number of inspections being undertaken it is evident that public authorities and law enforcement agencies in particular are making very effective use of communications data as a powerful investigative tool. Communications data has provided crucial evidence, which has led to the arrest and conviction of serious criminals e.g., kidnappers, rapists and paedophiles, and it is regularly used to combat organised and serious crime. The police and CSP work closely together to trace vulnerable or suicidal missing persons and this often results in the saving of life.

Interception successes

61. I have been impressed during my first nine months in office by how interception has contributed to a number of striking successes. It has played a key role in numerous operations including, for example, the prevention of murders, tackling large-scale drug importations, evasion of Excise duty, people smuggling, gathering intelligence both within the United Kingdom and overseas on terrorist and various extremist organisations, confiscation of firearms, serious violent crime and terrorism. I have provided fully detailed examples in the Confidential

Annex to this Report. I think it would be prudent, however, for the public to be assured as to the benefits of this highly intrusive investigative tool particularly in light of the current debate about whether or not intercept product should be used as evidence in a court of law. At present, I am firmly of the opinion that the benefits of any change in the law are heavily outweighed by the disadvantages, and with one exception, everyone to whom I have spoken in the course of my visits seems to be of the same opinion.

Conclusion

62. The interception of communications is, as my predecessors have already expressed in their Reports, an invaluable weapon for the purposes set out in section 5(3) of RIPA. It is my view that during 2006 interception played a vital part in the battle against terrorism and serious crime, and one that would have not been achieved by other means. I am satisfied that the intelligence and law enforcement agencies carry out this task diligently and in accordance with the law.

63. I have not in this report referred to the Wilson Doctrine but I adopt without qualification what was said about it by Sir Swinton Thomas last year. In times like these it seems to me to be totally indefensible.

64. My work would be impossible without the generous support not only of the Inspectors to whom I have referred but also of the small secretariat which works with me, with the Intelligence Services Commissioner and the Investigatory Powers Tribunal. I pay tribute to their excellent work.

65. Finally, it is clear from the first two paragraphs of this report that there is a mismatch between the starting date of the term of my appointment as Commissioner and the period to be covered by my first "annual" report. It seems to me that during my period in office thought should be given to the best way of resolving that anomaly.

Annex to the report of the Commissioner for 2006

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2006 and (b) issued during the period 1 April 2006 and 31 December 2006

	a	*b*
Home Secretary	754	1333
The total number of RIPA modifications from 01/04/2006 – 31/12/2006 = 3489		
Scottish Executive	43	102
The total number of RIPA modifications from 01/04/2006 – 31/12/2006 = 294		

[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 5714224 01/08 387082 19585

Printed on Paper containing 75% recycled fibre content minimum

ISBN 978-0-10-295183-7