Report of the Interception of Communications Commissioner for 2005-2006

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
19 February 2007

Laid before the Scottish Parliament by
the Scottish Ministers
19 February 2007

HC 315
SE/2007/17

Contents

From: The Right Honourable Sir Swinton Thomas

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

19 December 2006

I enclose my sixth, and final, Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. The Report covers my last fifteen months in office from 1 January 2005 to 31 March 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, the continued discharge of the functions of any public authority whose activities include activities subject to my review (section 58(7)) of the Act). Following the practice of my predecessor, I have taken the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published. I hope that this is a convenient course.

Sir Swinton Thomas

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

Annual Report of the Interception of Communications Commissioner for 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 sixth, and final, annual report as Commissioner and covers the period 1 January 2005 to 31 March 2006.

2. My successor as Commissioner, the Right Honourable Sir Paul Kennedy was appointed by the Prime Minister on 11 April 2006, and I warmly welcome his appointment. I agreed with Sir Paul to support him for a period in order to introduce him to the work and to complete my final annual report. Since 11 April 2006, Sir Paul and I have engaged together in 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, and we have, in addition, had a number of meetings with representatives of the Agencies to deal with issues that have arisen since his appointment.

3. I have followed the same practice as in previous years of giving as much information as I can in the first part of my Report. Over the past six years I have from time to time been subjected to criticism in the media for being over-secretive. I understand this criticism and, in many ways I would wish to be more open and transparent, but when dealing with work which is by its nature secret, that is not always possible. Balancing the requirements of secrecy with a desire for transparency is difficult to achieve. I am conscious that my Reports may appear to be bland, but I have made them as open as is possible in the circumstances, and this year the Report will be rather fuller on some issues than it has been in previous years. Those matters which cannot be fully explained without disclosing sensitive information relating to particular Agencies or to individuals concerned are contained in the Confidential Annex.

Functions of the Commissioner

4. The coming into force of the Regulation of Investigatory Powers Act 2000 (RIPA) on 2 October 2000 coincided with the coming into force of the Human Rights Act 1998 (HRA) which incorporated the European Convention on Human Rights into UK law. 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.

5. 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.

Discharge of my functions

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

(a) the exercise and performance by the Secretary of State of the power and duties conferred or imposed on him by or under sections 1 to 11;

(b) the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I;

(c) the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties conferred or imposed on him by or under Part III; and

(d) the adequacy of the arrangements by virtue of which:

(i) the duty which is imposed on the Secretary of State by section 15; and

(ii) so far as is applicable to information obtained under Part I, the duties imposed by section 55 are sought to be discharged.

7. These sections in RIPA set out the formal position of the post of the Commissioner for Interception of Communications. I work within that statutory context but the role is somewhat wider than that. It is not easy to summarise my role in short form, but essentially I see the role of Commissioner as encompassing these primary headings:

(a) To protect people in the United Kingdom from any unlawful intrusion of their privacy. This is provided for by Article 8 of the European Convention on Human Rights. I must be diligent to ensure that this does not happen, and alert to ensure that there are systems in place so that this does not and cannot happen. Over the long period that I have held my present post, I have found no evidence whatsoever of any desire within the Intelligence or the Law Enforcement Agencies in this field to act wrongfully or unlawfully. On the contrary, I have found a palpable desire on the part of all these Agencies to ensure that they do act completely within the four walls of the law. To this end, they welcome the oversight of the Commissioner and over the years have frequently sought my advice on issues that have arisen, and they have invariably accepted it. In any event, I believe that the legislation together with the safeguards and Codes of Practice that are in place make it technically virtually impossible to deliberately intercept a citizen's communications unlawfully with intent to avoid legal requirements.

(b) To assist the Agencies to do the work entrusted to them and, bearing in mind the number of organisations that I am now required to oversee, this occurs quite frequently. My work is, of course, limited to the legal as opposed to the operational aspects of their work. They take great care with their work and I have been impressed by its quality.

(c) To ensure that proper safeguards and Codes of Practice are in place to protect the public and the Agencies themselves. These have to be approved by the Secretaries of State. But every Secretary of State with whom I have worked has required to be informed as to whether the Commissioner has approved them before he or she is willing to do so.

(d) To advise Ministers, and Government Departments, in relation to issues arising on the interception of communications, the acquisition and disclosure of communications data, to approve the safeguards documents and the Codes of Practice.

The Growth in the Work

8. When I began in my post in April 2000, in the immediate wake of RIPA and the Human Rights Act, I had the nine Agencies and organisations empowered lawfully to intercept communications under section 6 of RIPA. Since then, as outlined in my previous Reports, I have, at the request of the Home Secretary, undertaken the inspection of interception in prisons, and on 5 January 2004 Chapter II of Part I of RIPA came into force enabling named organisations approved by Parliament to acquire communications data. The acquisition of communications data, although important and an extremely powerful and effective investigative tool, is not as intrusive as the interception of communications themselves. As at the date of this Report the number of organisations that I am required to inspect and oversee are as follows:

a. The nine Agencies as indicated above.

b. 52 police forces.

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

d. 139 prisons.

e. 475 local authorities authorised to acquire communications data.

f. 108 other organisations such as the Financial Services Authority, the Serious Fraud Office, the Independent Police Complaints Commission, the Ambulance Service and the Fire Service who are authorised to acquire communications data.

totalling 795 in all.

9. In addition I visit the principal Communications Service Providers in this field as reported below. The overall result of these additions is that the work of the Commissioner has changed and grown out of all recognition since I took up my post in April 2000. A new oversight regime is in place to deal with the increased workload, with the Commissioner retaining overall oversight, and I think I can report that the regime has settled down well and that proper oversight is already in place and working well. I deal more fully with this below.

10. It will be immediately apparent to any reader of this Report that 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 it was agreed with the Home Secretary that a Chief Inspector and the necessary number of inspectors would be recruited to carry out the bulk of the inspections in prisons and under Chapter II in respect of the acquisition and disclosure of communications data given the potential for intrusion into privacy albeit of a lesser kind than is the case in respect of communications content. All oversight under Chapter I continues to be carried out by the Commissioner alone. A recruitment exercise was undertaken through my sponsoring department, the Home Office. A recruitment agency was instructed, and there were a very large number of applicants. The applications had to be sifted and assessments made. This took a considerable time. Following the assessment, a number of applicants were interviewed by a panel of three, consisting of myself and two senior Members of the Home Office (the Head of my sponsor unit and an independent assessor). A Chief Inspector and five Inspectors were chosen, all with relevant experience from working in law enforcement or the private sector of using or interpreting communications data in criminal investigations and proceedings. The Chief Inspector was in post on 16 May 2005 and the remainder of the team joined between that date and 4 September 2005. Thereafter it was necessary for them to be trained in this work which included attendance at a residential course and the inspections commenced in the latter part of 2005. I will return to this aspect of the work later in this Report.

11. As recorded in last year's Report Part III of RIPA – providing for the disclosure of protected electronic data in an intelligible form or for disclosure of the means to access to make intelligible such – is not yet in force, but I understand that the Government is keeping this under urgent review and has subsequently undertaken a public consultation on a draft code of practice for Part III.

12. 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 (only visited once in this reporting period), the Police Service for Northern Ireland, the Northern Ireland Office, HM Revenue and Customs (HM Customs and Excise merged with the Inland Revenue and became HM Revenue and Customs on 1st April 2005), the Foreign and Commonwealth Office, the Home Office, the Scottish Executive (only visited once in this reporting period), and the Ministry of Defence. NCIS and the parts of HM Revenue and Customs which had responsibility for investigating drug trafficking have now become part of SOCA (the Serious Organised Crime Agency). In short, the intercepting agencies and 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 my previous visit. 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 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, when necessary, discuss the cases with the officers concerned. I can view the product of interception. It is of first 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.

13. 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 have 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 Department (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 and in those circumstances nothing I have examined in my view amounts to a criminal offence contrary to section 1 of RIPA or the statutory tort created by that section. If there is any product obtained through such errors it is immediately destroyed. The Agencies always make available to me personnel and documents requested by me. 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' anxiety to comply with the law. In case of doubt or difficulty, they do not hesitate to contact me and to seek advice, and I am sure that they will continue to contact my successor in the future.

14. During the year I met the Home Secretary on more than one occasion, the Foreign Secretary, the Secretary of State for Defence, the Secretary of State for Northern Ireland and the First Minister and 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 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".

15. In the course of the past year, 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 the Senior Executives in each company and 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 discuss the work that they do, the safeguards that are in place, any errors which have occurred, any legal or other issues which are of concern to them, and their relationships with the interception agencies. These meetings were particularly valuable at the outset of implementation of Chapter II when some of these organisations were having "teething problems" – now, I believe, happily resolved. Those who work in this field in the CSPs 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. It is of the greatest importance that nothing should be done which would detract from their enthusiasm and dedication (see below at paragraph 46vi).

16. In March 2005 I met officials from a Canadian Commission of Inquiry who were appointed to make recommendations to the Canadian government on a review mechanism for the national security activities of Canada's national police force, the Royal Canadian Mounted Police. The Commissioner leading the Inquiry was the Honourable Dennis O'Connor although he was not part of the team visiting the United Kingdom. My discussions with the Inquiry team were wide-ranging and fruitful.

17. In November 2005 I met a team of police officers from Turkey who were examining various issues relating to the interception of communications. The visit focussed on how the United Kingdom legislation works in practice, the methods of oversight and accountability, compliance with the Human Rights Act and the admissibility of intercepted material as evidence. The discussion I had with the officers provided an interesting insight and difference in procedures and practices.

18. With the Intelligence Services Commissioner, the Rt Hon Lord Brown of Eaton-under-Heywood, I attended the Intelligence and Security Committee in February 2006 for an informal discussion on our respective roles. With a new Chairman and new members, the Committee had changed significantly since my last informal discussion with them in December 2001. There was a frank exchange of views from both sides on a number of current issues.

Communications Data and the Work of the Inspectorate to Date

19. 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 and lifeboat services).

20. Those 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.

21. The objectives of the Inspectors are to ensure that communications data is being acquired in accordance with the Act and the 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 is adequate. In this way independent oversight is provided and good and bad practice is identified and fed back into the inspection process.

22. Since they commenced their inspections in the autumn of 2005, the Chief Inspector and the Inspectors have undertaken thirty-eight inspections of police forces and nine other law enforcement agencies, twenty-two inspections of local authorities and eighty three inspections of prisons. 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 five 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 which may run from about thirteen to about twenty-five typed pages. The Inspectorate has worked hard to achieve this in a comparatively short time and I hope that they will complete the inspections of all prisons and police forces and all local authorities who are making use of their powers by about the end of 2006. They have worked extremely hard to achieve what they have in such a short time and are to be congratulated.

Inspections of Police Forces

23. The Police Forces who had, before the introduction of RIPA, obtained communications data primarily through the service providers making disclosures under the Data Protection Act, took some time to all acclimatise 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 Code of Practice has been through several drafts and much consultation, and will be ready for approval by the Home Secretary shortly. In the initial stages there were some complaints that it was 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 Code of Practice, and now find that they are quite simple to comply with. Much work has gone into the preparation of the Code of Practice and the Home Office is to be congratulated on what it has achieved.

24. 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.

25. After the early teething difficulties the Inspectors found on the whole that the standard 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

26. As indicated in paragraph 8 above 475 Local Authorities are empowered to obtain communications data, of whom only 124 are making use of their powers, and of the 108 other public authorities, only 26 are using their powers. I am concerned that so many authorities who applied for the powers to be given to them, 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.

27. Inspections have taken place of all those authorities that are making significant use of their powers. Inevitably, the results have to an extent been variable. On the whole, however, we 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.

28. 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

29. 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.

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

31. 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.

32. 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 shown considerable improvement. I am reasonably confident

that in time inspections will show that there is total 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.

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, six 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.

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 80 new applications during the calendar year 1 January – 31 December 2005 and completed its investigation of 44 of these during the year as well as concluding its investigation of 49 of the 51 cases carried over from 2004. 38 cases have been carried forward to 2006.

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 2005.

Determination made in favour of complainants by Investigatory Powers Tribunal

39. During 2005 the Investigatory Powers Tribunal made a determination in favour of two complainants who lodged a joint complaint. This is the first time that the Tribunal has upheld a complaint. On the grounds of confidentiality, the Investigatory Powers Tribunal Rules 2000 prohibit me from disclosing specific details of the complaint, but it is sufficient to say that the conduct complained of was not authorised in accordance with the relevant provisions of the Regulation of Investigatory Powers Act 2000. The Tribunal ordered payment of an award of compensation to the complainants and the respondents to destroy the relevant records as provided for by section 67(7) of RIPA.

Safeguards

40. 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.

41. During 2005 I had sight of the revised handling arrangements produced by the Security Service. I provided my comments on this document which fully meets the requirements of section 15 of RIPA.

Section 17: Exclusion of Matters from Legal Proceedings

42. In my last Report I said that the question of the admission of intercept material in criminal proceedings had been discussed at some length in Parliament, the media and beyond. The aim of all concerned in the intercepting agencies is to use the material to best advantage to detect and prevent terrorism and serious crime. If it was a simple matter to change the law to allow intercept to be used evidentially without losing the very substantial benefits delivered by the existing intelligence only regime, I have no doubt that it would have been done many years ago. The truth is that there is no simple way of achieving this. I concluded by saying that I had no doubt that the balance of argument fell firmly against any change in the law, and that any change in the law, would, overall, be damaging to the work of the security, intelligence and law enforcement agencies.

43. I am still of that view, and it has been reinforced, and strengthened, by the events surrounding the London bombings and attempted bombings of 7th and 21st July 2005, and other terrorist enterprises, in respect of which I have had the opportunity and considerable advantage of seeing much material and having discussions with those involved. I propose in this Report to set out in a little more detail my reasons for taking the view that I do.

44. Various, in my view sometimes misguided, and often ill-informed, though no doubt well-motivated people continue to re-open this complex question. In order to understand it fully one needs a reasonably extensive knowledge of intelligence, law enforcement and the criminal process in Court. Amongst those who advocate changes are some lawyers, indeed some distinguished lawyers. They have, of course, an extensive knowledge of the law, and some, though certainly not all, a detailed knowledge of the criminal legal process. But they do not have knowledge of experience of intelligence and law enforcement work which is so vital in detecting and preventing terrorism and serious crime, and is a necessary prerequisite to putting criminals and terrorists in prison which is a prime objective of everybody concerned.

45. Those who advocate a change in the present law would be wise to discuss the issue with those who are knowledgeable on this subject. They do, after all, know what they are talking about. In my judgment, it is absolutely vital that anyone who wishes to pronounce on this topic should understand how technology changes will impact on their work.

46. It is impossible in Reports of this nature to discuss fully and in great detail my reasons for being firmly of this view in this complex area. But, put comparatively briefly, they are as follows;

i. If terrorists and criminals, most particularly those high up in the chain of command, know that interception would be used in evidence against them, they will do everything possible to stop providing the material which is so very valuable as intelligence. It is sometimes said: "but surely they know now that their communications will be intercepted?" They may suspect that their communications may be intercepted, but they do not know that they will be. This uncertainty is invaluable and they continue to provide immensely valuable intelligence material which would be lost if they ceased to communicate as they do now. Like everybody else they have to communicate to forward their enterprises, and there is a real danger that they will find means of doing so which are much more difficult or impossible to decipher if they know that the material would be used in evidence, so that valuable intelligence material leading to successful investigation and eventual prosecution will be lost. As has been widely publicised the Intelligence and Security Services have disrupted and prevented a number of serious prospective terrorist and criminal attacks both before and since July 2005. The intelligence derived from intercept has been crucial to these successes which might not have occurred if the intercept had not been available, as would be likely if those communicating believed that the material would be used in evidence against them. In addition to the advantages accruing from not knowing what intercepting agencies can do or are doing, it is a considerable advantage that they do not know what they are not doing or cannot do. All these advantages would be lost if all interception techniques are laid bare.

ii. Successive reviews on this subject over the last decade have been unable to show that the claimed benefits of using intercept product in evidence to secure more prosecutions (or to shorten trials) would be worth the risks that this entails for the operational effectiveness and capabilities of the agencies involved in fighting terrorism and serious crime. The last and most comprehensive review, the conclusions of which were reported in the then Home Secretary's written Ministerial Statement of 26th January 2005 found that a modest increase in convictions of some serious criminals, but not terrorists, would come with serious risks to the continued effectiveness of the agencies. The statement added that there was no immediate prospect of removing the main risks, partly because of the difficulty of lessening the impact of the major changes expected in communications technologies over the next few years.

iii. The workload for the intelligence and law enforcement agencies in preserving and presenting intercept product as evidence would be very severe indeed, and very expensive, and would distract them from the work which they should be doing, and also from the work they are actually doing, so greatly reducing as opposed to increasing the value of the intercept. This would be counter-productive. I give one example. In a recent case a Court felt it had to order that 16,000 hours of eavesdropping (not intercept) material must be transcribed at the request of the Defence. I believe that the cost was of the order of £1.9 million. The work and cost in intercept cases would be very great indeed, and quite disproportionate to any perceived advantage. This may explain why some who tend to act on behalf of defendants in terrorist and serious criminal cases appear to be supporting the concept of a change in the law.

iv. Criminals and terrorists do not speak in a language which is readily comprehensible to juries, even if their native language is English. Many conversations are in foreign languages or slang. In those that are not, they use their own particular language. In every case interpreters and translators would be required. In many languages and dialects there are very few capable of translating and interpreting. I give one example. In an intercept case which I saw recently, the participants were speaking in a tongue which is spoken by significantly less than 1000 people in the world.

v. Some of those who favour a change in the law take the view that if the terrorist or criminal makes a clear confession in a telephone conversation, then why should it not be admissible as evidence. That is an understandable point of view and the converse may at first sight seem to be counter-intuitive. However real life is not so simple as that and criminals and terrorists do not behave like that. Apart from the matters that I have already referred to, I know from years of experience, particularly when dealing with foreign languages that interpreters and translators very rarely agree upon the meaning of anything, and there is never any difficulty in finding one interpreter who will disagree with another.

vi. The Communications Service Providers (CSPs) are very important in this process and their staff do essential work. They are very co-operative and dedicated. I talk to them regularly and they are totally opposed to the concept of intercept being admissible in Court. The present regime provides a high degree of protection to the CSPs and particularly to those members of their staff who work in this sensitive field, and their strong co-operation referred to could easily be undermined. Here again, I think that it is essential for people holding views on this subject to talk to the CSPs, and to listen to what they say, and understand the basis of their strong opposition to any change in the present law.

vii. The problems with the criminal process. I have made some reference to these, with examples, above. Having looked at this problem with great care, it is abundantly clear to me that it would be exceedingly difficult to prove that a conversation is taking place between A and B. The warrants would have to be proved. How is the material received at source? How is it transferred to the Agencies? How is it transcribed? What does it mean? Lawyers will inevitably challenge every connection and every issue, because that is their job. Admitting intercept evidence would take a very long time, and would greatly increase the length of already over-long trials and the expense involved. These problems are going to increase in the future because of the huge changes taking place in telecommunications technology as CSPs change to internet protocol networks. There is a real danger of criminal trials being aborted. I know that work has been done in an

attempt to surmount these problems and the problems relating to European Community and Human Rights law, but I have not seen any system proposed which would successfully overcome these problems. The problems are very great and should not be understated.

viii. In conclusion, in my judgment, the introduction of intercept material in the criminal process in this country (other countries have different systems) would put at risk the effectiveness of the agencies on whom we rely in the fight against terrorists and serious criminals, might well result in less convictions and more acquittals and, most important of all, the ability of the intelligence and law enforcement agencies to detect and disrupt terrorism and serious crime and so protect the public of this country would be severely handicapped.

The Wilson Doctrine

47. On 17 November 1966, Mr Harold Wilson the then Prime Minister, made a statement in the House of Commons that there would be no tapping of the telephones of Members of Parliament but if there was any development of a kind which a change in the general policy, he would, at such moment as seemed compatible with the security of the country, on his own initiative, make a statement in the House of Commons. Subsequently, it has been confirmed that the Doctrine applies to all forms of communication, to Members of the House of Lords, and to electronic eavesdropping by the intelligence agencies. The Doctrine has remained in force ever since, and on 30 March 2006, the Prime Minister, Mr Tony Blair, said in answer to a question that the Wilson Doctrine would be maintained. It is an issue which falls squarely within the responsibilities placed on the Interception of Communications Commissioner by Parliament by Section 57 of the Regulation of Investigatory Powers Act 2000.

48. The Doctrine may have been defensible when it was first enunciated in 1966 when there was no legislation governing interception and there was no independent oversight. In 1966 there was no requirement for a warrant with all the safeguards that are attached to that operation now.

49. Now, in 2006, the interception of communications is the primary source of intelligence in relation to serious crime and terrorism and is strictly regulated. The Doctrine means that MPs and Peers can engage in serious crime or terrorism without running the risk of being investigated in the same way as any other member of the public. In the course of many meetings I have had with Ministers and Members of Parliament, it has become clear that many are determined that that state of affairs should continue.

50. It is fundamental to the Constitution of this country that no-one is above the law or is seen to be above the law. But in this instance, MPs and Peers are anything but equal with the rest of the citizens of this country and are above the law.

51. Some MPs may fear that the situation now is the same as it was in 1966 when it was at least theoretically possible for the Executive to intercept communications for its own purpose but it is not, for the following reasons –

i. For there to be interception, there must be a Warrant in place, signed by the Secretary of State authorising the interception.

ii. The grounds for doing so are very limited by Section 5(3) of the Act. They are essentially National Security (including terrorism) and the prevention or detection of serious crime.

iii. There is oversight by the Commissioner to prevent wrongful use, and I have made it clear that the Commissioner would personally ensure that there was no improper interception of the communications of any public figure.

iv. It is important to appreciate that in reality it is impossible to achieve the interception of a telephone conversation by a Government Agency without a Warrant and the safeguards attached to it. So those who support the retention of this particular privilege have nothing to fear unless they are engaging in terrorism or serious crime.

v. The interception of communications is the most important investigative tool in the investigation of serious crime, such as fraud, drug smuggling, the downloading of child pornography, sexual offences with minors and perjury. Of course, I do not think that Members of Parliament are engaging in serious crime and terrorism. Indeed I have the greatest respect for our democratic institutions. However to maintain that no MP or Peer ever has or ever will engage in serious crime is absurd.

vi. Nonetheless it is clear to me that a number of Ministers and many MPs from the Speaker of the House of Commons downwards, who I have spoken to on this subject, are determined to maintain this privileged status.

52. There are three further important points to be made:

i. The Security Services and Law Enforcement Agencies are not remotely interested in acquiring personal information about Members of Parliament or, indeed, other citizens, except in strict observance of their statutory functions. Moreover, for the reasons set out above, it would not be possible for them to do so. I can say this with confidence after six years in my current post. It is also very important to remember that most investigations of serious crime are carried out at least in substantial part, by interception.

ii. It is in truth all but impossible for an intercepting agency to intercept telephone conversations unlawfully by deliberate means. Interception of the communications of a citizen by an intercepting agency can only take place with a Warrant based on serious crime or national security grounds. Before a Warrant can be granted, it must be shown that there is evidence already in place that the person concerned is involved with serious crime or terrorism. It has to be considered by senior departmental officials and, if deficient, it is rejected at that stage. It then goes to the Secretary of State. It would, in my experience, be inconceivable and exceedingly dangerous for him or her to sign a Warrant on improper grounds. And, finally, in this context, it will be seen by the Commissioner who must ensure that no improper interception takes place. It is also worth noting that since 1994: a.) all three intelligence agencies operate under statute; b.) they are overseen by the parliamentarians of the Intelligence and Security Committee and the Intelligence Services Commissioner both of whom are independent of government; c.] they are subject to a complaints procedure under the independent Investigatory Powers Tribunal; and that d.] Sections 2(2)(b) and 4(2)(b) of the Intelligence Services Act 1989 and Section 2(2)(b) of the Security Service Act prevent those services from taking "any action to further the interests of any political party".

53. When he made his statement in the House of Commons on 13 March 2006, the Prime Minister was kind enough to make reference to the advice that I had given to him to the effect that the Wilson Doctrine was at the present time in the changed circumstances unsustainable. I understand, and have sympathy with the Prime Minister in the circumstances in which he was placed, namely strong opposition within the Cabinet and in the House of Commons to any change in the current position. I recognise that ending the Doctrine might put pressure on the Prime Minister to disclose whether the prohibition of telephone tapping of Members of Parliament has been maintained since 1966 and, if not, to make a statement on the circumstances of its ending. I do not consider that this is any

argument to the contrary. I have no doubt that the Prime Minister could readily deal with this issue particularly bearing in mind Section 19 of the Regulation of Investigatory Powers Act which requires that interception matters shall be kept secret.

54. What is more difficult to understand is the basis of opposition apart from self-interest or, possibly, lack of understanding, in the maintenance of a privilege enjoyed by nobody else, given that there are perfectly adequate safeguards in place that serve MPs and non-MPs alike. In the conversations that I have had with Ministers and members of Parliament on this issue, I have not been able to find any logical, and, certainly not, any principled objection to change apart from self-interest. After this issue received some media publicity earlier this year, a number of people have spoken to me, both within and outside legal and intelligence circles, and the reaction has been one of astonishment and incredulity that this situation should be allowed to continue.

55. To the best of my knowledge, there is no other country in the world that provides the privilege to its elected representatives and Peers to be immune from having their communications lawfully intercepted with the accompanying advantage that they may be immune from criminal investigation and prosecution.

56. The Wilson Doctrine applies to MPs and Peers but cannot apply to Members of the European Parliament or Members of the Scottish Parliament or Members of the Welsh or Northern Ireland Assemblies. It is plainly right that it should not but it provides a striking illogicality.

57. In my view the Doctrine flies in the face of our Constitution and is wrong. I do not think that it provides MPs with additional protection. I think in fact that it is damaging to them.

Errors

RIPA Part I Chapter I: Interception

58. A significant number of interception errors and breaches have been reported to me during the course of the period of this report – 66 in all. This reflects an increase of 22 on the 45 errors reported during 2004. The number of errors is unacceptably high. It should, however, be stressed that, as any reader of this report will readily understand, there have been periods of time in the course of the last eighteen months when the relevant Intelligence and Law Enforcement Agencies have been working under extreme pressure, with some employees working round the clock. At times such as these it is more likely, and more understandable, that mistakes may be made. 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., 1945 instead of 1954. 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.

59. The **Home Office** reported one error which occurred in relation to the revalidation of an emergency warrant modification. The revalidation request was received in the Home Office on the afternoon before it expired at midnight. However, it was not actioned until the following day as the request was not highlighted as being a revalidation of an emergency warrant modification which expired on that day and therefore required urgent attention. Despite this the telephone line was not cancelled and remained active until revalidated. No product was received between the expiry time and the time the modification was revalidated.

60. The **Scottish Executive** also reported one error where a warrant schedule

contained, through a typing error, an incorrect telephone number: a single digit within the number being incorrectly inserted. The Scottish Executive has reviewed its processes with staff being reminded of the steps that must be taken to ensure accuracy in all warrantry paperwork.

61. The **Northern Ireland Office** reported nine errors of which four 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.

62. In two 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 the product was destroyed. In both cases, the correct numbers were added to their respective warrants.

63. Seventeen errors were reported to me by **GCHQ** of which five are highlighted below. The first case arose out of avoidable human error. A target whose calls were being intercepted lawfully was found to be in the United Kingdom. The target's change of location escaped the attention of the analyst who failed to take any action either to stop listening to the calls or obtain further authorisation. None of the calls were transcribed and all have been deleted.

64. The second error occurred in relation to a request made of GCHQ to intercept the communications of an individual whilst he was overseas. The target traveled overseas but returned the same day. When he left the UK his details were added to GCHQ's databases for his communications to be intercepted. Unfortunately, it was not removed on his return to the UK and remained on the database for a further three weeks. During this period one item of 2 seconds duration was intercepted but was deleted as being of no interest. GCHQ will devise procedures to help prevent a recurrence.

65. Another similar error occurred during the report period. A customer requested GCHQ to intercept the communications of an individual whilst he was overseas. Once he had left the UK, the target's details were added to GCHQ's databases for his communications to be intercepted. Unfortunately the number was not removed from the database for five days following the target's arrival back in the UK. During this time fifty items were selected, half of which had been listened to. No calls were transcribed. Again, GCHQ will devise procedures to help prevent a recurrence.

66. The fourth error arose out of a mistake by a new member of staff at GCHQ. The agency was asked for assistance in providing information on an individual who was in the UK. No interception was requested. A newly-deployed analyst entered the individual's details on GCHQ's targeting database for information purposes only. In error the target's details were entered onto GCHQ's databases for interception. On discovery of this action the address was immediately removed. Fortunately, no material had been selected. This was a human error. The analyst was moved from this section and no longer uses the targeting database.

67. In the fifth case, GCHQ entered the details of a target known to be overseas into databases in order to intercept his communications. Unfortunately, when requesting that this number be intercepted, the GCHQ analyst mistyped the number by transposing two digits within the correct number. No intercept resulted; either the number was not active or had not been allocated to a subscriber. In the absence of intercept, GCHQ did not investigate further as this may have involved an unnecessary invasion of privacy. The analysts have been reminded of the importance of double-checking the accuracy of the telephone numbers.

68. The **Security Service** reported seventeen errors. Brief details of six are highlighted below. The first case relates to postal intercepts against three addresses. On the vacation of the targets from two premises, the addresses should have been deleted from the warrant. This has now been done. No mail for

individuals other than those covered by the warrant was intercepted. Security Service staff have been reminded of the importance of maintaining comprehensive records of the status of communications addresses covered by warrants.

69. Five separate errors occurred when the Security Service sought modification of warrants to add new telephone numbers. Due to human error digits were either transposed or mistyped and incorrect numbers added to the schedules to the respective warrants. On discovery the numbers were deleted from their respective schedules. In four of the cases no product was received and in the fifth case what product was received has been destroyed. Security Service staff have been reminded of the importance of carrying out thorough checks of telephone numbers added to interception warrants.

70. The **Secret Intelligence Service** reported one error when their mail room sent warrant documents meant for one communications service provider (CSP) to another. In normal circumstances, the SIS mail room puts correspondence for a CSP in envelopes which bear a label addressed to that CSP. These envelopes are then put inside a plastic pouch which also bears a label addressed to the same CSP. The breach occurred because the inner envelopes were correctly addressed to the CSP whilst the outer envelope was addressed to a completely different CSP. New checking procedures have been instigated in the SIS mail room to prevent a future recurrence.

71. **HM Revenue and Customs (HMRC)** reported three errors. In the first case, HMRC made an application for a warrant against a telephone number which was authorised and interception commenced. Concern was expressed about the lack of product. A check revealed that HMRC's application to the Home Office showed three different digits in the telephone number. Interception ceased immediately: as already mentioned no product was received. It appears that the three last digits of the telephone number were transposed as the final print of the application was made prior to its submission to the Home Office. Manual checks of the final print are now made in HMRC to prevent future recurrences.

72. The second error occurred in the authorisation of a modification to the schedule of an interception warrant. A telephone number was identified for a target which HMRC sought to have added to a schedule to an interception warrant. Following authorisation, interception of the number commenced but it became apparent from the product that the mobile telephone was not in the possession of the target. A check of the paperwork revealed that a typographic error had been made in the intelligence report upon which HMRC had acted: this resulted in the identification of the incorrect mobile telephone number. The intercept was suspended immediately. HMRC reinforced its procedures for checking source data used in all applications.

73. The third error reported by HMRC was one not of their making nor the communication service provider. A series of computer upgrades were undertaken, some of which were not successful. The unsuccessful upgrades resulted in intercept product which was not relevant to the warranted telephones being intercepted. This incorrectly delivered product was occasionally interspersed with correctly delivered product relevant to the particular telephone. Whilst the majority of the product delivered incorrectly was attributable to other telephones warranted by HMRC, there was at least one instance where the intercept product was believed to relate to another agency. These delivery faults were reported and were rectified with intercept product subsequently being delivered correctly.

74. The **National Criminal Intelligence Service** reported three errors. An example of one of NCIS's errors is when they sought modification of a warrant to add a new telephone number. Due to human error a digit was mistyped and an incorrect number added to the schedule to the warrant. On discovery the interception was suspended and the number deleted from the schedule. No intercept product was received. NCIS has made improvements to their procedure to prevent a recurrence of a similar error.

75. I now turn to give three examples of the fourteen errors made by the **Communications Service Providers (CSPs)**.

76. The first, reported by the Secret Intelligence Service, concerned warrantry paperwork. The CSP incorrectly sent warrantry paperwork for a cancelled warrant to a government department instead of back to SIS for destruction.

77. The second, reported by the Northern Ireland Office, relates to a CSP intercepting the wrong mobile telephone number. The correct number was passed to the CSP but the company mistakenly intercepted a number one digit higher.

78. The third error was reported by the Security Service. Product from an interception revealed that the target intended seeking a new home telephone number. On being given a new number, the CSP automatically continued intercepting before receiving the warrantry paperwork for the new number. The Security Service suspended the intercept on the original number immediately and added the new number to the schedule to the warrant. No calls to the new number were monitored or transcribed before it was added to the schedule.

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

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

80. 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 inquiry. In such circumstances the Public Authority must destroy the data as soon as it has made its report to my office.

81. Public Authorities also have a responsibility to report any errors which are made by Communications Service Providers (CSPs) in the course of acquiring 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.

82. During the period covered by this report 3,972 errors were reported to my office. A total of 2,712 of these errors were attributable to CSPs and the remainder (1,260) 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 439,054 during the same period. **I have concluded that no useful purpose would be served in giving further details about the individual errors in this report.** There are two reasons for this. First, as I have already indicated, the inspections are not yet complete 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. My successor may well, of course, take a different view in subsequent reports. 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.

83. 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 is not relevant. 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.

84. From the inspections 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 kidnappers, rapists and paedophiles, and it is regularly used to combat organised and serious crime. The Police and Communications Service Providers work closely together to trace vulnerable or suicidal missing persons and this often results in the saving of life.

Interception successes

85. During the period of this Report, interception continued to contribute to a number of striking successes. Fully detailed examples have been provided in the Confidential Annex. I do feel, however, that the public may like 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.

86. Interception 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. As to be expected, substantial use was also made of interception and communications data in the investigation of the bombings in London in July 2005. The product obtained enabled significant successes to be achieved in the fight against terrorism.

Conclusion

87. I have said in my previous Reports and earlier in this Report that the Interception of Communications is an invaluable weapon in the continuing battle against terrorism and serious crime. The work in this field has become ever more technical and difficult, and will continue to do so. At the conclusion of my period in office, I would like to stress in this, my last Report, that I have been very impressed by the care and very hard work which Ministers, the Intelligence and Law Enforcement Agencies, and the civil servants working in this field, give to this work to ensure that it is carried out properly and in accordance with the law. I would also wish to thank them for the help and support that they have given to me, and their willingness to accept any advice that I may give or criticism that I may make.

88. I would also like at the end of my tenure to pay tribute to the very hard working and very loyal staff in the Office of the Interception of Communications Commissioner.

Annex to the report of the Commissioner for 2005-2006

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 March 2006 and (b) issued during the period 1 January 2005 and 31 March 2006

	a	*b*
Home Secretary	553	2243
The total number of RIPA modifications from 01/01/2005 – 31/03/2006 = 4746		
Scottish Executive	43	164
The total number of RIPA modifications from 01/01/2005 – 31/03/2006 = 397		

[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 5524545 02/07 361081 19585

Printed on Paper containing 75% fibre content minimum.

ISBN 978-0-10-294450-1