Report of the Interception of Communications Commissioner for 2001

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
31 October 2002

Laid before the Scottish Parliament
by the Scottish Ministers
October 2002

HC 1243
SE/2002/300

£6.50

Report of the Interception of Communications Commissioner for 2001

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
31 October 2002

Laid before the Scottish Parliament
by the Scottish Ministers
October 2002

HC 1243
SE/2002/300

Contents

From: The Right Honourable Sir Swinton Thomas

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

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

Dear Prime Minister

I enclose my second Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. It is, of course, for you to decide, after consultation with me, how much of the report should be excluded from publication on the grounds that it is prejudicial to national security, to the prevention or detection of serious crime, to the economic well-being of the United Kingdom, the continued discharge of the functions of any public authority whose activities include activities subject to my review (section 58(7)) of the Act). Following the practice of my predecessor, I have taken the course of writing the report in two parts, the confidential annex containing those matters which in my view should not be published. I hope that this is a convenient course.

Sir Swinton Thomas

Annual Report of the Interception of Communications Commissioner for 2001

Introduction

I was appointed the Interception of Communications Commissioner on 11 April 2000 under the provisions of the Interception of Communications Act 1985, and as from 2 October 2000 under section 57 of the Regulation of Investigatory Powers Act 2000. This is my second annual report as Commissioner which covers the year ending 31 December 2001.

2. I have followed the same practice as in previous years of giving as much information as I can in the first part of my Report. Those matters that cannot be fully explained without disclosing sensitive information relating to particular agencies or to individuals or the organisations concerned are contained in the confidential annex.

Functions of the Commissioner

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

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

- To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 7 to 11 of RIPA and the adequacy of any arrangements made for the purpose of sections 15 and 16 of RIPA.
- To keep under review the exercise and performance by the Secretary of State of the powers and duties conferred or imposed by or under Chapter II of Part I (the acquisition and disclosure of communications data).
- To give the Investigatory Powers Tribunal set up under section 65 of RIPA all such assistance as the Tribunal may require for the purpose of enabling them to carry out their functions under that section. I give further information about the Tribunal in paragraphs 62 to 64 below.

Discharge of my functions

5. In my first report last year I referred in some detail to the impact of the enactment of the Regulation of Investigatory Powers Act 2000, and the incorporation of the European Convention on Human Rights into the law of the United Kingdom had on the interception of communications generally, and on government agencies concerned with interception, and on my consequent duties referred to above. I also said that in this year's Report I would give a more detailed assessment of the impact of this legislation and I do so later in the Report.

6. In accordance with these duties I have visited the Security Service, the Secret Intelligence Service, GCHQ, the National Criminal Intelligence Service, the Special Branch of the Metropolitan Police, the Strathclyde Police, the Police Service for Northern Ireland (formerly the Royal Ulster Constabulary), HM Customs and Excise, the Foreign Office, the Home Office, the Scottish Executive and the Ministry of Defence at least twice during 2001. I have been very impressed by the quality and the dedication and the 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 strive assiduously to comply with the statutory criteria and, in my view, there is very little, if any, danger that an application which is defective in substance will be placed before the Secretary of State. Where errors have occurred, which I refer to below (and in detail in the confidential annex) these have been errors of detail and not of substance. Where errors occur they are reported to me and if there is any product it is immediately destroyed. The agencies have made available to me everything that I have wished to see or hear about in conformity with the statutory duty placed upon them. They welcome the oversight of the Commissioner, both from the point of view of seeking his advice, which they do quite frequently, and as a reassurance to the general public that their activities are overseen by an independent person who has held high judicial office. I am also left in no doubt as to their anxiety to comply with the law. In a case of doubt or difficulty, they do not hesitate to consult me.

7. Prior to each visit to the agencies I obtain a complete list of the warrants issued or renewed since my previous visit. I then select, largely at random, a sample of warrants for close inspection. In the course of my visit I satisfy myself that the warrants satisfy the requirements of RIPA, that proper procedures have been followed, that the relevant safeguards and codes of practice have been followed. In the course of my visits I review each of the files and the supporting documents and discuss the cases directly with the operational officers concerned. I can view the product of the interception. It is important to ensure that the facts justify the use of interception in each case and those concerned with interception fully understand the safeguards and the codes of practice.

8. During the year I have seen the Home Secretary, the Foreign Secretary, the Secretary of State for Northern Ireland, the Secretary of State for Defence and the First Minister for Scotland. Again, I have been impressed with the care that they take with their warrantry work to ensure that warrants are issued only in appropriate cases and, in particular, in ensuring that the conduct authorised is proportionate to what is sought to be achieved by the interception.

9. I have also visited the Communications Service Providers (CSPs), that is to say the Post Office (now known as Consignia) and all the major telephone companies. In the course of my visits, I was impressed by the care, interest and dedication of their employees to their work in this field, and their understanding of the need at all times to comply with the safeguards imposed on them. This is of the greatest importance.

10. Many members of the public are suspicious about the interception of communications, and some believe that their own conversations are subject to unlawful interception by the security, intelligence or law enforcement agencies. To an extent this may be understandable, because people do tend to be suspicious of what takes place in secret, and are worried by the "big brother" concept. Interception for lawful purposes, of course, and inevitably, takes place in secret. In my oversight work I am conscious of these concerns. However, I am as satisfied as I can be that the concerns are, in fact, unfounded. Interception of an individual's communications can take place only after a Secretary of State has granted a warrant and the warrant can be granted on strictly limited grounds set out in Section 5 of RIPA, essentially the interests of national

security and the prevention or detection of serious crime. Of course, it would theoretically be possible to circumvent this procedure, but there are in place extensive safeguards to ensure that this cannot happen, and it is an important part of my work to ensure that these are in place, and that they are observed. Furthermore, any attempt to get round the procedures which provide for legal interception would, by reason of the safeguards, involve a major conspiracy within the agency concerned which I believe would, for practical purposes, be impossible. I am as satisfied as it is possible to be that deliberate unlawful interception of communications of the citizen does not take place. I say "deliberate" because on rare occasions technical errors do occur which may render an interception unlawful in which case the product, if any has been received, from the interception is always destroyed.

The Extent of Interception: General

11. As in the past, the Annex to this Report contains a summary of the numbers of warrants in force at the end of 2001 and those issued throughout the course of the year by the Home Secretary and the Scottish First Minister. The great majority of warrants issued in England and Wales and Scotland remain related to the prevention and detection of serious crime. The continuing incidence of serious and organised crime and an increased facility to counter it are the main cause of the larger numbers of warrants. The significantly high level of warrants sought each year, with a corresponding level of workload for the Secretaries of State and on the part of the relevant Agencies, clearly calls for the exercise of vigilant supervision. I can report that the level of scrutiny has been and continues to be generally well maintained. However I remain concerned about the number of errors reported during the year. It is inevitable that in any detailed, technical human activity errors may occur. I have impressed on the agencies the need to eliminate errors or, at least, to reduce them to an absolute minimum. The agencies are very aware of the importance of this, and on each occasion where an error has occurred they review their procedures with a view to ensuring that the same error does not recur. Keeping errors to a minimum is one of the reasons for having the safeguards in place. I will, of course, continue to monitor the system to satisfy myself that every effort is being made to prevent such recurrences and seeking full explanations where these systems fail.

The Extent of Interception: Scotland

12. There was some criticism of the level of the interception of communications in the year 2000 in Scotland in the Scottish Parliament and the Scottish media in February 2002. My inspections in Scotland show quite clearly that warrants for interception there have been granted by Ministers in Scotland only in cases which properly fall squarely within the definition of serious crime and within the upper echelons of that definition.

Regulation of Investigatory Powers Act 2000: impact of the legislation on the work of warrantry units in government departments and the security, intelligence and law enforcement agencies

13. During my visits to the security, intelligence and law enforcement agencies I have discussed the impact that the implementation of RIPA has had on their work. As before, I have highlighted in the confidential annex some examples of the agencies' experience of the new legislation. I think it would also be helpful for me to give in this part of my Report a more detailed account of the impact on the agencies of the legislation as perceived by them.

Foreign and Commonwealth Office

14. The Regulation of Investigatory Powers Act (RIPA) tightened the rules governing interception in two key areas: (i) warrants are now required to be issued against a named individual as opposed to an address or telephone number, and (ii) the Secretary of State is now explicitly required by the Act to be content that the action authorised under the warrant is proportionate to the product of that action.

15. RIPA has not added to the FCO's workload, but it has reinforced the existing requirement within the FCO to ensure that warrants from the agencies requiring the approval of the Foreign Secretary pass strict quality control criteria. The proportionality requirement leads all involved in providing advice to the Foreign Secretary to be fully engaged in the warrantry application process, and in all cases making a firm recommendation based on fully weighted argument.

Home Office

Advantages

16. The change in warrants from being address specific to being person specific has eased the burden on the Secretary of State. He has been required to consider and authorise 1314 warrants in 2001 as opposed to 2080 in 2000. The task has been removed from the Home Secretary in relation to amending warrants (modifications) and this is now undertaken by Senior Officials.

17. After initial teething troubles and staff problems the issue of warrants, but in particular modifications, is now dealt with more speedily. In practice, however, the rise in applications (approximately 15%) has eaten up a good deal of the headroom the Home Office expected to be created.

18. All warrants are now authorised for an initial period of three months and renewed at three monthly intervals (serious crime) and six monthly intervals (national security and economic well being). This has again reduced the time staff have had to spend on renewal applications with the consequent saving in staff time and resources.

19. The provision allowing urgent modifications with a limited lifespan to be made by a Head of Agency, or nominated deputy who is expressly authorised by the warrant, has meant a speedier implementation of interception.

20. The fact that agencies are now nominated on a warrant rather than Public Telephony Operators has meant a considerable saving in paperwork and administration costs for those in the Home Office who deal with warrantry applications but significantly increased that of the agencies.

21. The new legislation will enable security, intelligence and law enforcement agencies to match their investigative techniques with continuously changing new techniques.

22. The legislation sets out clearly for the first time those agencies permitted to carry out interception activities.

Disadvantages

23. The Home Office sees no particular disadvantages flowing from RIPA.

Scottish Executive

24. The level of interception in Scotland has increased markedly since the introduction of RIPA. The main factor for this increase appears to be the targets' propensity to change mobile telephones with incredible frequency (for

which RIPA makes adequate provision by permitting modification by senior officials). This has led to a commensurate increase in the volume of the Scottish Executive's paperwork, and while the modification procedure has removed much of the bureaucratic burden from Ministers, they are adapting their working arrangements to cope with the demands arising from this aspect of RIPA. They are, however, closely monitoring the increases in interception to ensure that each individual application (whether a new application or modification) meets the strict criteria specified in the Act. This remains the most important aspect of their interception procedures.

25. The Scottish Executive's overall view is that the mechanisms for the interception of communications are more efficient, but there is no doubt that the volume of paperwork generated by the new procedures places considerable demands on their Warrants Unit.

Northern Ireland Office

26. During the year the Northern Ireland Office handled a significant volume of transactions under the new legislation. In general they found the processing of warrant modifications to be speedier under RIPA. This is particularly helpful in counter terrorism and serious crime (drugs) casework in which targets, for operational and security reasons, make frequent changes of their mobile telephones. Speed of response is essential in enabling the police to maintain intercept coverage of their targets. The ability to seek emergency authorisations through specified officials has also eased the process. In the context of serious crime the Northern Ireland Office have found it beneficial to have warrants operated for three months compared to one month previously, thereby reducing the bureaucratic workload on staff dealing with revalidations on a monthly basis.

Ministry of Defence

27. The MOD and HM Armed Forces undertake a wide range of interception of communications in support of GCHQ and during the conduct of their own military operations overseas. The former are authorised by warrants obtained by GCHQ.

Government Communications Headquarters

28. GCHQ considers that a major advantage of RIPA is that it focuses the mind of the Secretary of State on the target and requires that he must consider the proportionality of the proposed course of action: subordinate details, such as the telephone number used by the target is in the schedule part of the warrant and remains subject to careful scrutiny as under the previous arrangements. RIPA (and the implementation of the Human Rights Act) provided the impetus for a thorough examination of GCHQ's handling processes. Whilst this led to some minor rationalisation, it is the case that there has been no real reduction in paperwork or bureaucracy - either for GCHQ officials or those in the FCO who normally deal with warrant applications and modifications and who scrutinise the scheduled parts of the warrants. The greater and more extensive formality of the procedures involved has brought some additional costs in terms of effort devoted to them by staff in Operations. However, GCHQ is unable to quantify this and there has been no adverse impact on the production of required intelligence.

29. It may be of interest to know that prior to the coming into force of RIPA and the Human Rights Act 1998 in October 2000, GCHQ undertook extensive preparatory work to ensure that the requirements laid upon the agency were fully understood and met. These included the establishment of RIPA/human rights strategy and working groups to develop the new processes and staff training needed and to ensure that these were implemented successfully.

30. A project was also established to provide the technical support to reinforce the requirement for all interception to be properly reviewed to ensure that it remained justified. The project also addressed the auditing of systems to demonstrate post hoc whether an individual has or has not been the subject of action by GCHQ and, if so, that this was authorised, justified and proportionate. The project evaluated a large number of systems: technical modifications were made to a small number and procedural controls were recommended for others.

31. In addressing the safeguards contained within section 15 of RIPA, GCHQ developed a new set of internal compliance documentation for staff, together with an extensive training programme that covered staff responsibilities under both RIPA and the Human Rights Act. This compliance documentation was submitted to the Foreign Secretary who was satisfied that it described and governed the arrangements required under section 15. I have also been told it also constituted the written record of the arrangements required to be put in place by the Director, GCHQ, under section 4(2)(a) of the Intelligence Services Act 1994 (to ensure that no information is obtained or disclosed by GCHQ except so far as is necessary for its statutory functions). In discharging my functions under section 57(1)(d), I examined the documentation and the processes which underpin it and satisfied myself that adequate arrangements existed for the discharge of the Foreign Secretary's duties under section 15 of RIPA. Of course, GCHQ recognises that its compliance processes must evolve over time, particularly as they become more familiar with the intricacies of the new legislation and develop new working practices, and that the process of staff education remains a continuing one. To this end, GCHQ has developed further training programmes and is issuing revised compliance documentation as part of the ongoing process (see also under paragraph 56 under Safeguards).

32. In advance of the coming into force of RIPA, GCHQ approached me as to the warrants it would seek after that date and provided a detailed analysis as to how those warrants would be structured - this was helpful as it gave me an insight into how GCHQ saw the workings of RIPA/Human Rights Act and permitted me to comment in advance. Since the commencement of RIPA, in reviewing warrants I have looked carefully at the factors to be considered by the Secretary of State when determining whether to issue an interception warrant, and especially the new requirement to consider "proportionality" under section 5(5)(2)(b) of RIPA.

Security Service

Implementation: General

33. The Security Service welcomed the introduction of RIPA, having taken an active part in its drafting. However, it found that the process of changing arrangements for warrantry and internal authorisations, as required by the Act, required a considerable re-allocation of resources within the Service. Staff attended Home Office working groups which considered the various aspects of the legislation and its implementation. Internal working and steering groups were necessary to consider the practical effects of the new arrangements on working practices in the Service. An initial far-reaching training programme was devised and delivered. There is a continuing programme of training for new entrants to the Service and refresher training for existing staff, including managers. The warrantry unit was expanded to cover the additional paperwork and the provision of advice to staff.

RIPA Part I, Chapter I - Interception of Communications

34. **Change 1:** unlike the Interception of Communications Act 1985 (IOCA) warrants, which were served on the communications service provider (CSP), warrants obtained under RIPA Part I are served on the organisation which has applied for the warrant. The legislation requires the CSP to assist in carrying out warranted intercepts.

35. **Change 2:** under RIPA Part I, the same warrant may cover all the communications of an individual. There are, therefore, more modifications to warrants (additions and deletions) but fewer new applications and cancellations than before.

> **Advantage:** given the range of communications often possessed by one individual, the new arrangements are easier to manage. One subject has only one warrant and this will require just one renewal. Under IOCA, warrants for intercepts with different CSPs, depending on the timing of their imposition, could be renewed at different times, adding to the workloads of desks, line management, and the warrantry unit.

> **Advantage:** given that modifications may be authorised by Home Office senior officials and not just the Home Secretary, (and given that the former are likely to be more available) the interception of new lines can be put in place more quickly.

> **Advantage:** emergency modifications may be authorised by the Director General, Deputy Director General or Service Legal Adviser. Again, given that they are likely to be more quickly available, in emergencies, the interception of new lines can be put in place more speedily.

36. **Change 3:** the interception of private telecommunications networks (for instance in a hotel) could not be warranted under IOCA. This meant that it was possible for someone whose private network conversations had been intercepted to argue that his or her privacy had been invaded unlawfully. Under RIPA, all cases of "private side" interception need warranting.

> **Advantage:** the warranting provides compliance with ECHR.

37. **Change 4:** under IOCA, some kinds of communications (for instance, those involving certain internet service providers) could not be warranted. RIPA Part I has been drafted so that new ways of communicating should all be able to be warranted.

> **Advantage:** subjects of Security Service investigations are making increasing use of e-mail and other relatively recent technologies. RIPA clarifies the legal position of their interception, and provides ECHR compliance.

38. **Change 5:** interception of pager messages need to be warranted under RIPA Part I.

> **Advantage:** once again, RIPA clarifies the legal position.

> **Disadvantage:** there is a delay whilst the warrant is obtained.

39. **Change 6:** all RIPA Part I warrants other than those obtained under emergency procedures will be valid for three months initially and for six months (national security) or three months (serious crime) following each subsequent renewal.

> **Advantage:** increase in duration for initial authorisations for both national security and serious crime warrants, and increase in subsequent duration of the latter following renewal, is a widely felt advantage. This results in less paperwork for intelligence sections and the warrantry unit.

Secret Intelligence Service

40. In SIS's view, the drafting and enactment of RIPA provided a useful opportunity to modernise the warrantry system developed under the

Interception of Communications Act, making it more effective and efficient in response to the changing nature of today's communications environment. RIPA also offered an opportunity to legislate for the interception of communications other than those offered by public telecommunications operators and the Post Office, which are being used increasingly by SIS targets (particularly internet communications). When the legislation is fully enacted, SIS will be able to extend and improve its interception capabilities against priority targets.

41. The main advantages are:

- Quicker arrangements for modifying the telephone numbers being targeted. Rather than seeking the signature of the Secretary of State for amendments or new warrants for each communications service provider (CSP) used by the target (as under the Interception of Communications Act), schedules can now be modified by a designated senior official. This improves their coverage of targets who are increasingly switching their communications systems between CSPs.

- Extended renewal period for warrants on the prevention or detection of serious crime grounds (now three months instead of one). This allows for better assessment of the product and of the justification for renewal of the warrant. It also reduces the administrative burden.

- More efficient urgency procedures (although SIS has not yet needed to deploy them). In urgent circumstances, schedules may now be modified in-house, rather than obtaining oral authority from the Secretary of State, which was required to modify an Interception of Communications Act warrant.

42. RIPA has not required SIS to make significant changes to its handling procedures for safeguarding intercepted material. Only a small amount of updating has been required to ensure full compliance with RIPA.

Metropolitan Police Special Branch

43. The new legislation was eagerly anticipated at the MPSB, who have traditionally had to deal with sophisticated targets using a variety of communications methods that the previous legislation, the Interception of Communications Act, could not adequately cope with.

44. In the view of MPSB there is a disadvantage inherent in the enhanced flexibility for coping with new technology in that RIPA requires more paperwork and, most importantly, an individual agency itself now has to process this greatly expanded paperwork. MPSB has found this quite difficult where the staffing of the warrants unit underscores the recognition that interception is a relatively minor, albeit important, activity compared with other forms of surveillance or with their other core functions such as ports and protection work.

45. MPSB are unable to say whether their warrantry caseload has increased under RIPA, as this was already on a rapidly rising wave before RIPA came into force in October 2000. The trend has continued since then. MPSB recognises that RIPA has enabled them to respond more swiftly to changes in their targets' communications although they do not believe that it has led to an increase in actual targeting.

46. Despite a slightly hesitant start, when it appeared to MPSB to be more straightforward to obtain a new warrant than an amended schedule, things have now settled down to a more balanced arrangement.

47. Extending the renewal interval from one month to three for serious crime warrants has been of great benefit to MPSB and its customers. The extended period is much more realistic in enabling MPSB to properly assess the intelligence developed in connection with any particular target. Statistically, MPSB warrants are now held for longer than in the past - typically over a period of several months rather than days. However, this is a reflection of their new approach to this type of work rather than a factor inspired by RIPA.

HM Customs and Excise (HMCE)

48. Changes in the warrantry administration system have been vital for HMCE being able to maintain their effectiveness against targets using disposable pre-paid mobile telephones.

- Although modifications to the warrant were possible under the Interception of Communications Act 1985, it was still a legal requirement that the Home Secretary authorised all applications. RIPA now permits a senior Home Office official to authorise modifications to warrants, and consequently the processing of warrants should be much quicker. The two or three week delay in the Home Office processing modifications earlier this year - which negated the benefits of RIPA - has now improved: increased staffing levels has enabled processing to take place within satisfactory timescales.

- A particularly important benefit has been the ability of HMCE officials to modify warrants in urgent cases, particularly out of hours. This system enabled them to respond quickly and has resulted in some major seizures of class A drugs together with a number of arrests.

- The administration burden involved in the monthly renewal of warrants has been greatly reduced due to warrants being extant for three months rather than one, and only one warrant per target now being necessary as opposed to one warrant per telephone under the Interception of Communications Act 1985.

- However, I understand that the administrative burden has increased on HMCE's staff because they now have responsibility, as opposed to the Home Office, for the service of warrants and schedules on the communication service providers. Nonetheless, HMCE view the administration system under RIPA as being much speedier and more effective and efficient.

National Criminal Intelligence Service

49. In general the impact on NCIS has been beneficial and where there has been extra burden this has been due to a reallocation of responsibility from other areas of government. The extra burden has not been inordinate.

Warrantry

50. The main benefit for NCIS has been the change in the warrantry regime, which warrants an individual rather than a device. This has benefited NCIS in particular as most of their targets frequently change their communications devices and also carry several at one time. The modification procedure is much quicker and allows NCIS to keep up the intelligence flow.

51. A broad comparison between the year preceding RIPA and the year since shows that prior to RIPA, NCIS had just over 600 warranted target addresses. In the year after they had about 800 target addresses deriving from only just over 400 warrants. This represents a significant increase in target coverage with a reduction in warrantry which has in turn meant that the time taken in warrantry has also reduced, further enhancing coverage.

Service of warrants

52. The main extra responsibility for National Criminal Intelligence Service is the service of warrants. This function was devolved from the Home Office.

53. Another side effect of the change is that agencies now have to keep copies of the warrants, application documents and renewal documents. These documents often contain intercept product and have to be shown to the prosecutor on request. This allows them access to intercept product that they did not have before.

Overall

54. The responses of the Agencies are, I think, interesting and enlightening. Whereas, of course, there were safeguards in place under IOCA, and the same care was taken with the warrantry process as now under RIPA, the latter together with the Human Rights Act have caused the Agencies to review all their procedures. There are now in place Safeguards and a Code of Practice which ensure, so far as it is possible, that the principles and practice laid down in the two Acts are complied with. The Code of Practice was introduced into Parliament on the 8th May 2002 and debated on the 21st May, and came into force on 1st July 2002. In the Parliamentary debates it was generally welcomed, in particular the clarification of the meaning of the economic well being of the United Kingdom.

55. I agree with the views expressed by the Agencies that RIPA and the Human Rights Act, whilst to some extent increasing the paperwork and manpower involved, have modernised the warrantry process, reinforced the concept of proportionality, and, whilst not in any way decreasing the efficiency of the interception of communications process, has strengthened the system for the protection of the rights of the citizen.

Safeguards

56. 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 dissemination, disclosure, copying, storage, and destruction etc., of intercepted material. These sections require careful and detailed safeguards to be drafted by each of the agencies referred to earlier in this Report and for those safeguards to be approved by the Secretary of State. This had been done. I have been impressed by the care with which these documents have been drawn up, reviewed and updated in the light of technical and administrative developments. Those involved in the interception process are aware of the invasive nature of this technique, and care is taken to ensure that intrusions of privacy are kept to the minimum. There is another incentive to agencies to ensure that these documents remain effective in that the value of interception would be greatly diminished as a covert intelligence tool should its existence and methodology become too widely known. The sections 15 and 16 requirements are very important. I am satisfied that the agencies are operating effectively within their safeguards.

Codes of Practice

57. Section 71(a) of RIPA requires the Secretary of State to issue one or more Codes of Practice relating to the exercise and performance of duties in relation to Parts I to III of the Act. The Home Secretary, having first obtained my views and interim approval of the draft Code of Practice prepared by the Home Office gave his approval to the draft Code on the basis that he wished to see an updated Code of Conduct at a later date when RIPA had been in force for a time. The Home Secretary has consulted me in relation to an updated Code of Practice which was prepared by the Home Office in consultation with the relevant agencies and has been approved by the Home Secretary.

Communications data

58. Chapter II of Part I of RIPA applies to the acquisition and disclosure of Communications Data. Section 57 of the Act requires me to keep under review the exercise and performance by the persons on whom they are conferred or imposed these powers and duties. Chapter II of Part I is not yet in force. It was anticipated that it would come into force in October 2001, but for various reasons the commencement date has had to be postponed. When it does come into force it will involve a very substantial increase in my duties as the Commissioner. In addition to the Ministries and Agencies that I oversee at present in relation to the interception of communications it is anticipated that 64 Police Authorities and an as yet uncertain number of Public Authorities will be authorised to acquire and disclose communications data. Oversight will of necessity involve visits to those concerned with this work and a very considerable extension of the Commissioner's work. It will not be possible for me to undertake this work without assistance and the extent and nature of the assistance that I will require is being considered by the Home Office in consultation with me and my staff.

Prisons

59. I have been asked by the Home Office, and have agreed in principle, to oversee the interception of communications in prisons. This has not come into effect in the year 2001 which is the subject of this Report but will come into effect in 2002 with a corresponding increase in the volume of work, the provision of assistance to me in carrying out oversight, and an increase in my staff.

Staffing of the Secretariat

60. In my last Report I said that the situation in relation to my staff had been unsatisfactory for a period of time. I am happy to be able to report that this problem has been cured. Much of the backlog of work has been cleared and I believe that the staffing of the Commissioners and the Tribunal is now working smoothly.

Foreign and Commonwealth Office and Northern Ireland Office warrants

61. In paragraphs 10 - 12 of my predecessor's 1995 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 outline the reasons behind this decision.

62. 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 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."*

63. 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 March 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.

The Investigatory Powers Tribunal

64. The Investigatory Powers Tribunal was established by section 65 of the Regulation of Investigatory Powers Act 2000. The Tribunal came into being on 2 October 2000. From that date the Investigatory Powers Tribunal assumed responsibility for the jurisdiction previously held by the Interception of Communications Tribunal, the Security Service Tribunal and the Intelligence Services Tribunal and the complaints function of the Commissioner appointed under the Police Act 1997 as well as claims under the Human Rights Act. The President of the Investigatory Powers Tribunal is Lord Justice Mummery with Mr. Justice Burton acting as Vice-President. In addition, seven senior members of the legal profession serve on the Tribunal. During 2001 a Registrar was appointed to help in the process of hearing claims alleging infringements of the Human Rights Act.

65. As I explained in paragraph 25 of my first report last year, complaints to the Investigatory Powers Tribunal cannot be easily "categorised" under the three Tribunal system that existed prior to RIPA. Consequently, I am unable to detail those complaints that relate solely to the interception of communications. I can only provide information on the total number of complaints made to the Investigatory Powers Tribunal. The Investigatory Powers Tribunal received 102 new applications from the day of its formation on 2 October 2000 to the end of December 2001. The Tribunal completed its investigation of 71 of these during the year. 31 cases have been carried forward to 2002. On no occasion has the Tribunal concluded that there has been a contravention of the Regulation of Investigatory Powers Act 2000 or the Human Rights Act 1998.

Assistance to the Investigatory Powers Tribunal

66. 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 have not had occasion to give any assistance to the Tribunal in 2001.

Errors

67. A significant number of errors and breaches have been reported to me during the course of the year - 43 in all. By way of example, details of some of these are recorded below. It is important from the point of view of the public that I should stress that none of the breaches or errors were deliberate, that all were caused by human or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. Most did not involve any breach of RIPA as such. The most common cause of error is a

simple transposition of numbers by mistake e.g. 3142 instead of 3124. The examples that I give are typical of the totality and are anonymous. Full details of the errors and breaches are set out in the Confidential Annex.

68. One administrative error occurred at the Home Office. The issue of a new schedule to authorise the interception of a landline was sought but the Home Office obtained the signature to a modification of an existing schedule. Fortunately the intercept was still in the process of being set up; it was immediately suspended. The Home Office subsequently obtained authorisation for the issue of a new schedule.

69. The Security Service reported a total of nine errors. In one case, an error occurred when an existing warrant, that was modified under the emergency procedures, was not renewed or suspended within the required timescale i.e., five days. The relevant investigative section in the Service decided not to renew the intercept and asked that it be suspended by the section responsible for providing the transcription. Unfortunately, a communication breakdown occurred between the sections resulting in the Service receiving product until the error was finally noticed 4 days later. The intercept was immediately suspended and the product destroyed, none of which had been transcribed. The mistake was originally the result of a lack of communication between these two sections within the Security Service with the breach not being reported and addressed in a timely and effective way. I understand that the staff in the sections concerned have been reminded of the importance or reporting breaches promptly and clearly so that a repetition can be avoided.

70. The second error occurred in a warrant that covered the interception of two landlines and a mobile telephone. The three lines covered by the warrant were suspended. The mobile telephone line was then deleted from the warrant as it had not been producing intelligence of interest prior to suspension. The two landlines were not deleted at this time for operational reasons. The two landlines were subsequently re-imposed but when this was done the check on the mobile telephone was also re-imposed in error at the communications service provider at the Security Service's behest. This reveals that both the CSP and the Security Service were at fault. Although the Security Service incorrectly advised the CSP to re-impose the mobile telephone line, the CSP should not have done so as there was no schedule in place to cover the interception. During the period until the error was discovered three calls were intercepted. Although these calls were listened to, nothing was transcribed and all the calls have been erased from the Security Service's recording system.

71. The third error occurred in the case of a postal intercept address being added to a warrant. Before the Security Service requested the addition of the address to the warrant they confirmed with the CSP that the address was accurate. Consequently, the address was added to the warrant. Subsequent enquiries with the CSP established the correct postcode for the address, a code that was different to that on the warrant. Once the error was discovered the postal intercept was suspended and a modification sought to delete the address from the warrant. The addition of the correct address was not sought, however, and as the other address details were correct no mail to anywhere other than the target address was intercepted.

72. Four of the remaining six errors involved separate warrants containing incorrect telephone numbers; individual digits within the numbers being transposed incorrectly. On discovery, the unlawful intercepts were immediately suspended. In two cases product was received but it was not transcribed. The product was immediately destroyed. In the third case no calls were intercepted. The fourth was different in that it represented a technical breach of RIPA for although there was a mistaken transposition of digits on the modification form, the intended number was intercepted as it had been passed correctly to the communications service provider.

73. The final two errors again occurred on separate warrants. In the first case there was a failure to suspend a postal check pending its deletion from a warrant. In the second case it was the result of an official failing to sign the modification authorisation to a warrant.

74. Twelve errors were reported by GCHQ, of which four are highlighted below. In the first case the CSP noticed that the Schedule to a warrant that was sent to them contained a wrong number. The CSP informed GCHQ immediately and no targeting or interception of the number took place. Modification deletion instruments to remove the number were subsequently signed. Checks are always made to ascertain subscriber details for numbers being proposed for targeting but on this occasion the error was not spotted. In light of this, GCHQ has reviewed its internal working arrangements.

75. In another case a modification instrument was signed adding an additional number to a warrant Schedule held by a CSP authorising the interception of mobile telephone numbers. However, staff in GCHQ noticed that the modification to add an additional number to the CSP's Schedule was, in fact, the first of that CSP's number on this warrant. The modification should, therefore, have constituted a modification to insert a new Schedule (in respect of the CSP) and should have been accompanied by the Schedule addressed to that CSP, together with a requirement for assistance notice. As soon as this error was noticed, steps were taken to prevent the number in question from being intercepted. One call had been intercepted but had not been listened to: this data was immediately destroyed. Corrected paperwork was subsequently submitted. It appears that this error arose out of simple oversight when drawing up the modification instruments. GCHQ has revisited its procedures for ensuring that appropriate checks are made in this aspect of the submission process.

76. The third case concerned modification instruments to add numbers to two of GCHQ's existing warrants. The modifications were signed and distributed to the two relevant CSPs. On receipt of the instruments both CSPs informed GCHQ that the instruments they each had received contained telephone numbers of the other CSP. The CSPs did not take the actions necessary to enable interception to be carried out. GCHQ took the appropriate action to rectify the errors. Further investigations by GCHQ revealed that numbers owned by the two CSPs had been incorrectly assigned to modification instruments within GCHQ's warrant database and that manual checks had failed to spot these errors. GCHQ are in the process of amending the warrant database to prevent a recurrence of such errors in the future.

77. The fourth case concerned the intercept from a targeted number which had been dual-routed to both GCHQ and SIS. SIS expressed concern to GCHQ that the target was no longer using the particular mobile telephone number under interception. Investigations within GCHQ confirmed this fact. Interception was terminated at once. Modification deletion instruments were submitted to delete the number from the warrant. Enquiries of the CSP established that the target had cancelled his mobile telephone and, as is normal practice, the CSP held the number in "storage" for four months before re-allocating it to a new subscriber. A period of unlawful interception therefore took place. There were, in total, 184 intercepts of this number: none were looked at by GCHQ and none were transcribed. All have now been deleted. GCHQ's internal procedures have been reviewed and actions taken to prevent a similar error arising again.

78. Two incidents were reported to me by the Northern Ireland Office. The first concerned an error in the interception of a mobile telephone used for the purposes of national security. Intelligence received indicated that the target

intended changing his mobile from one CSP network to another. The appropriate warrant was modified to delete the old number and to add the new number. The new intercept did not produce any product during the first few days of its operation. The mobile telephone was not being used and therefore no calls were intercepted and transcribed. It also transpired that the telephone number had been mis-reported by the source of the intelligence and that one digit was wrong. Intercept of the mobile was suspended immediately and the warrant modified to operate against the correct mobile telephone number. Although everyone involved in this case acted in good faith, consideration is being given to whether routine procedures can be put in place to confirm the subscriber to a mobile telephone whenever that information is available.

79. The second was a report of a breach of security for which the Northern Ireland Office was not responsible and which is detailed more fully in the confidential annex. This is currently the subject of an investigation by the Belfast Special Branch.

80. The National Criminal Intelligence Service reported three errors. The first case involved the targeting of "third criminal" whose services were thought to be used in a kidnap. A warrant was obtained for a mobile telephone with no subscriber details. When the first product of the interception was received it was clear the target under interception was not the "third criminal". A check revealed an error had been made and the facility was immediately suspended then cancelled. No product was recorded. The correct facility was then acquired by way of an urgent modification. An investigation revealed that the wrong telephone number had been forwarded within NCIS. NCIS has inserted an additional checkback process in their procedures.

81. The second error concerned the warrant issued to target a known criminal. The warrant authorised the interception of the target's home and mobile telephone numbers as well as another telephone number used by the target. From this latter interception NCIS officers became aware of a new mobile telephone number for the target. A modification to the new warrant to add this mobile telephone was obtained and interception commenced. However, it became clear from the first call intercepted that the telephone was not in the possession of the target. An investigation revealed that the telephone number of one of the investigating police officers was forwarded to be included in the modification rather than the target's number. The interception was suspended and monitoring ceased. The wrong number was cancelled with the PTO and the correct number added to the warrant. Unlawful interception occurred for less than one day and arose out of human error. Arrangements have been put in hand within NCIS to ensure no recurrence of similar errors.

82. In the third case, an interception warrant was obtained for a mobile telephone of a known criminal. However, shortly after interception commenced it became clear that the target had discarded the telephone in favour of another. The line was rightly cancelled with the CSP. The Home Office was advised and with a request that the interception be cancelled. It was indicated that the operational team would make another application when a new facility was identified. A new number was subsequently identified and with the agreement of the Home Office a Director's modification was issued. A ratification report was subsequently submitted to the Home Office and it was at this point that it was discovered that the warrant had been cancelled as a result of an earlier report from NCIS. The new facility was immediately cancelled with the CSP, a fresh warrant issued and lawful interception commenced. I understand that this breach has discussed between the Home Office and NCIS and in future where a warranted target is not the subject of current interception the report will be specifically titled to ensure that the problem does not recur.

83. Two errors are attributable to NCIS. In both cases the telephone numbers that had been targeted and intercepted turned out to be the wrong numbers. Human error was responsible. In the first case the mistake was one digit in an eleven-digit number and in the second, a wrong number was provided to the National Crime Squad by an overseas police force.

84. I now turn to give four examples of the fifteen errors made by the communication service providers (CSP). The first occurred when a CSP employee wrongly assumed that a warrant had been signed and made a connection to the targeted line. Having discovered the breach the Security Service suspended the check on its internal systems and notified the CSP of the error. The calls were not transcribed and the intercept product was destroyed. I understand that the CSP has admitted the mistake, which was caused by human error, and will endeavour to prevent it from happening again.

85. The second case involved an error made by members of a CSP who made preliminary arrangements to provide intercept of a telephone line at the same time as an application for the issue of a schedule to authorise this intercept was being processed by the Home Office. Although a connection had been made no product was received by the targeting agency.

86. In the third example product from a Security Service interception warrant was incorrectly addressed and delivered by a CSP secure courier service to the Metropolitan Police Special Branch (MPSB). On opening the envelope and discovering that the material was not for them the MPSB contacted the CSP and the product was resealed and returned to the CSP for onward transmission to the correct agency.

87. The final example concerns a modification which was signed to delete a number on a line that was unproductive. The CSP was telephoned by the FCO and informed of the modification. The CSP interpreted the telephone call as an instruction to provide interception of that number, which they duly did, and telephoned GCHQ to confirm this. Realising what had happened, GCHQ contacted the CSP who immediately removed the line from their interception system. No interception took place. This is the first error of this type experienced; it arose from a verbal misunderstanding between the CSP and the FCO and occurred during a very busy period. The matter has been discussed with all those involved and the importance of making telephone instructions very clear has been stressed.

88. The remaining eleven errors fall into three categories. There were six cases where unauthorised product was received by the agencies due to technical and/or engineering problems at the CSPs. All product received by the agencies was immediately destroyed. In a further three cases, interception was set up on wrong telephone numbers by the relevant CSPs. The product relating to the incorrect numbers was destroyed immediately and no material disseminated in any form. The remaining two cases concerned two CSPs who supplied intercept material to the targeting agencies for new numbers that had not been included on a modifications to the warrants' schedules. All unlawful product received was destroyed.

89. No errors were reported by the Secret Intelligence Service, the Metropolitan Police Special Branch and HM Customs and Excise. No specific errors have been reported by the Ministry of Defence, but they have reported one technical breach of RIPA which I have dealt with in more detail in the Confidential Annex.

Conclusion

90. The interception of communications is an invaluable weapon for the purpose set out in section 5(3) of RIPA and, in particular, in the battle against terrorism and serious crime. The task of the agencies working in this field has become much more difficult and complex as a result of the proliferation of mobile telephones and the greater sophistication of criminals and terrorists. RIPA brought the legislation up to date in the light of new developments in technology in the communications industry, such as e-mail, satellite telephones, radio pagers and the like and the proliferation of mobile telephones. An individual warrant may permit the interception of the person named in the warrant or named premises. The law was simplified in relation to the implementation of warrants, the issue of emergency warrants, their duration and their discharge. These changes have increased the efficiency of the enforcement agencies and the speed with which, in appropriate circumstances, they may act but in each case they are covered by section 15 safeguards.

91. The Security Service have reported to me that the interception of communications is of invaluable assistance to their work. Over the past year intelligence gained from interception warrants has contributed to a number of successful operations both in the Service's work on national security and its work on serious crime, where it acts in support of law enforcement agencies. Intelligence gained from interception warrants has helped the Service's investigation of international terrorism in the aftermath of the events of 11 September 2001.

92. GCHQ report that during the period of this report interception has continued to play a critical role in promoting and protecting vital UK national interests including the fight against terrorism, combating serious crime and supporting UK forces deployed overseas.

93. The Metropolitan Police Special Branch tell me that since the enactment of RIPA in October 2000 almost half of their operations involving interception of communications have resulted in the arrest and prosecution of persons engaged in serious criminal activity, and in many of the other cases the intelligence obtained has led to the disruption of the criminal enterprises of the targets and their close associates. Since the 11th September there has been a significant increase in the operations conducted by MPSB, all of which have been directed against threats to national security and serious crime involving individuals, groups and organisations based in this country.

94. HM Customs and Excise tell me that interception is a crucial time-critical tool which enables the investigation and intelligence arms within the Department to meet the targets set for them by the Government and make Government strategies in the fight against Class A drugs and large scale tax evasion work.

95. I have no doubt that in 2001, as before, interception has played a vital part in the battle against terrorism and serious crime, and one which would not have been achieved by other means. I am also confident that Ministers and the intelligence and law enforcement agencies carry out this task in accordance with the law.

Annex to the report of the Commissioner for 2001

Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2001 and (b) issued during the period 1 January 2001 and 31 December 2001

	a	b
Home Secretary	464	1314
The total number of RIPA modifications from 01/01/2001 - 31/12/01 = 1788		
Scottish Executive	43	131
The total number of RIPA modifications from 01/01/2001 - 31/12/01 = 194		

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

Printed in the UK for The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID118959 10/02 065536

ISBN 0-10-291834-1

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

Online
www.tso.co.uk/bookshop

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

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

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

TSO Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 010 291834 1