Report of the Interception of Communications Commissioner for 2007

Commissioner:
THE RT HON SIR PAUL KENNEDY

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
22 July 2008

Laid before the Scottish Parliament by
the Scottish Ministers
July 2008

HC 947
SG/2008/127

£5.15

Report of the Interception of Communications Commissioner for 2007

Commissioner:
THE RT HON SIR PAUL KENNEDY

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
22 July 2008

Laid before the Scottish Parliament by
the Scottish Ministers
July 2008

HC 947
SG/2008/127

£5.15

ISBN: 978 0 10 295736 5

Contents

From: The Right Honourable Sir Paul Kennedy

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

27 June 2008

I enclose my second Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. The Report covers the period 1 January 2007 to 31 December 2007. 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 predecessors, I have taken the course of writing the report in two parts, the Confidential Annex containing those matters which in my view should not be published. I hope that this is a convenient course.

Sir Paul Kennedy

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

Annual Report of the Interception of Communications Commissioner for 2007

Section 1: General

Introduction

1.1 On 11 April 2006 I was appointed the Interception of Communications Commissioner under Section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). My appointment is for a period of three years.

1.2. I am required by section 58(4) of RIPA as soon as practicable after the end of each calendar year to report with respect to the carrying out of my functions as the Interception of Communications Commissioner. This is my second annual report as Commissioner and it covers the period 1 January 2007 until 31 December 2007. In producing my report, I propose to follow, as my predecessors have done, the practice of writing the report in two parts, this main part for publication, the other part being a Confidential Annex to include those matters which cannot be fully explained without disclosing sensitive information.

Functions of the Commissioner

1.3 I was appointed under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). The coming into force of RIPA on 2 October 2000 coincided with the coming into force of the Human Rights Act 1998 (HRA) which incorporated the European Convention on Human Rights into UK law. These two important pieces of legislation brought about a number of changes in the law and in the practice of those responsible for the lawful interception of communications.

1.4 As Commissioner I have four main functions: these are set out in section 57 of RIPA and, for ease of reference, are as follows:

- To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 1 to 11 of RIPA and the adequacy of any arrangements made for the purpose of sections 15 and 16 of RIPA.
- To keep under review the exercise and performance by the Secretary of State of the powers and duties conferred or imposed by or under Chapter II of Part I (the acquisition and disclosure of communications data).
- To keep under review 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 (investigation of electronic data protected by encryption etc).
- 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

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

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

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

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

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

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

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

are sought to be discharged.

1.6 Part III (sections 49 to 56, together with Schedule 2) of RIPA – investigation of electronic data protected by encryption etc) – contains provisions designed to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal and hostile intelligence use of encryption (the means of scrambling electronic information into a secret code of letters, numbers and signals). Encrypted information cannot be unscrambled without a decoding key. Part III introduces a power to require disclosure of protected (encrypted) data. Parliament has now approved the Code of Practice for the investigation of protected electronic information; it came into force on 1 October 2007 and provides guidance for the authorities to follow when they require disclosure of protected electronic information.

Section 2: Part I Chaper I – Interception of Communications

General

Oversight arrangements

2.1 I have decided to continue with the practice followed by my predecessors of making twice yearly visits to the Security Service, the Secret Intelligence Service, Government Communications Headquarters, the Serious Organised Crime Agency, the Metropolitan Police Counter Terrorism Command, Strathclyde Police, the Police Service for Northern Ireland, the Northern Ireland Office, HM Revenue and Customs, the Foreign and Commonwealth Office, the Home Office, the Scottish Executive and the Ministry of Defence. In short, I meet officers in the agencies undertaking interception work and officials in the departments of the Secretaries of State/Ministers which issue the warrants. Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since 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 criteria of RIPA, that proper procedures have been followed and that the relevant safeguards and Codes of Practice have been followed. During each visit I review each of the files and the supporting documents and discuss the cases with the officers concerned. I can, if I need to, view the product of interception. It is of paramount importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

2.2 I have been impressed by the quality, dedication and enthusiasm of the personnel carrying out this work. They possess a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards. All applications made to the Secretary of State are scrutinised by officials in the warrants unit within their respective

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. If there is any product obtained through such errors it has been immediately destroyed. The Agencies always make available to me personnel and documents that I have requested. They seem to welcome my oversight, as ensuring that they are acting lawfully and appropriately, and they seek my advice. It is a reassurance to the general public that their activities are overseen by an independent person who has held high judicial office. I am left in no doubt at all as to the Agencies' commitment to comply with the law. In case of doubt or difficulty, they do not hesitate to contact me and to seek advice.

Meetings with the Secretaries of State

2.3 During the period of this Report I met the Home Secretary, the Foreign Secretary, the Secretary of State for Defence and the Secretary of State for Northern Ireland. I was unable to meet the First Minister for Scotland but I did, however, meet the Justice Minister who, in reality, signs most of the warrants in 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 and proportionality are not met. The agencies are well aware that the Secretary of State does not act as a "rubber stamp".

Visits to the communication service providers and internet service providers

2.4 During 2007, I visited a total of ten communications service providers (CSPs) and internet service providers (ISPs) consisting of the Royal Mail and the communications companies who are most engaged in interception work. These visits, mostly outside London, are not formal inspections but are designed to enable me to meet both senior staff in each company as well as the personnel who carry out the work on the ground, and for them to meet and talk to me. I have no doubt that the staff in the CSPs and ISPs welcome these visits. We discussed the work that they do, the safeguards that are in place, any errors that have occurred, any legal or other issues which are of concern to them, and their relationships with the interception agencies. Those in the CSPs and ISPs who work in this field have great enthusiasm; 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.

Intelligence and Security Committee

2.5 Along with the Intelligence Services Commissioner, Sir Peter Gibson, I attended the Intelligence and Security Committee on 1 May 2007 for an informal discussion about our respective roles. There was a helpful exchange of views on a number of current issues including the work of the agencies, errors, the admissibility of intercept as evidence and the Wilson Doctrine.

Privy Council Review of Intercept as Evidence

2.6 On 25 July 2007 the Prime Minister announced a Privy Council Review of Intercept as Evidence under the chairmanship of Sir John Chilcot. I attended the committee as a witness on two occasions – the first when I met Sir John Chilcot himself in August 2007, the second was in November 2007 when I met and talked to the whole committee. I have read their Report (published on 30 January 2008:

CM 7324) and the statement made by the Prime Minister to the House of Commons on 6 February 2008 accepting the committee's main conclusion that it should be possible to find a way to use some intercept material as evidence provided – and only provided – that certain key conditions can be met. The report sets out nine conditions in detail. They relate to complex and important issues, and include: giving the intercepting agencies the ability to retain control over whether their material is used in prosecutions; ensuring that disclosure of material cannot be required against the wishes of the agency originating the material; protecting the current close co-operation between intelligence and law enforcement agencies; and ensuring that agencies cannot be required to transcribe or make notes of material beyond a standard of detail that they deem necessary.

2.7 The committee acknowledged that further extensive work is needed to see whether and how these issues and other conditions – intended to protect sensitive techniques, safeguard resources, and ensure that intercept can still be used effectively for intelligence – can be met. This is a recommendation that the government has accepted. I understand that a detailed implementation plan will be developed under which material might be made available for use in criminal cases in England and Wales, strictly subject to all the Chilcot conditions being met. I welcome the government's acceptance that if the Chilcot conditions could not be met then intercept as evidence should not be introduced. I will watch the development of the implementation plan with interest.

International Symposium: Accountability of Intelligence and Security Agencies and Human Rights

2.8 On 7 and 8 June 2007 I attended an International Symposium in The Hague, The Netherlands. The theme of the Symposium was "the accountability of the intelligence and security agencies and human rights". Members of the Intelligence and Security Committee were also present. There were delegates from a number of countries from around the world – including Belgium, Canada, Czech Republic, Germany, The Netherlands, Norway, Poland, South Africa, Sweden, United Kingdom and the United States of America. With the intelligence and security services assuming an ever more important role – they have the power to infringe universally acknowledged human rights, subject to strict conditions – the Symposium discussed what these conditions were and how oversight in this context is organised from the perspective of human rights instruments such as the European Convention on Human Rights (ECHR). A number of sessions looked at themes related to the Symposium topic from the perspectives of (i) oversight bodies, (ii) the academic community, (iii) the judiciary, (iv) the media and (v) the intelligence and security services themselves. I found the discussions during the Symposium and in the course of informal meetings to be interesting, informative and valuable.

Successes

2.9 I continue to be impressed as to how interception has contributed to a number of striking successes during 2007. It has played a key role in numerous operations including, for example, the prevention of murders, tackling large-scale drug importations, evasion of Excise duty, people smuggling, gathering intelligence both within the United Kingdom and overseas on terrorist and various extremist organisations, confiscation of firearms, serious violent crime and terrorism. I have provided fully detailed examples in the Confidential Annex to this Report. I think it is very important that the public is re-assured as to the benefits of this highly intrusive investigative tool particularly in light of the on-going debate about whether or not intercept product should be used as evidence in a court of law.

Errors

2.10 Twenty-four interception errors and breaches have been reported to me during the course of 2007. This is the same number of errors reported in my first Annual Report (which was for a shorter period) and is a significant decrease in the number reported by my predecessor. I consider the number of errors to be

too high. By way of example, details of some of these errors are recorded below. It is very important from the point of view of the public that I stress that none of the breaches or errors were deliberate, that all were caused by human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. The most common cause of error tends to be the simple transposition of numbers by mistake e.g., 1965 instead of 1956. The examples that I give are typical of the totality and are anonymous so far as the targets are concerned. Full details of all the errors and breaches are set out in the Confidential Annex.

2.11 The **Northern Ireland Office/Police Service Northern Ireland** reported four errors. In one case, an incorrect telephone number was cited on the warrant due to the transposition of digits but no product was received.

2.12 Six errors were reported to me by **GCHQ** of which three are highlighted below. The first case involved an analyst mistyping a telephone number into GCHQ's targeting database. During the period the number was the subject of interception no calls to or from the telephone were intercepted. The analyst has been reminded of the importance of accuracy in entering numbers into the targeting database.

2.13 The second error occurred during a fast paced incident. Because of the urgency of the situation the telephone number provided by an official source was accepted in good faith and the number added to an existing warrant by a senior official. Unfortunately when a sample of the calls was analysed they were found to have no intelligence value and to involve conversations between two unidentified people. Consequently, the calls that were recorded were deleted from GCHQ's systems.

2.14 The third error was caused by a technical problem with an automated process which resulted in an instruction to remove two numbers due for deletion not being passed to all GCHQ's call collection systems. Other numbers deleted from the same warrant at the same time were successfully removed. The computer software controlling this process has subsequently been improved.

2.15 The **Security Service** reported eight errors. Brief details of three of these are highlighted below. In the first case the Security Service processed a modification to add a new mobile telephone number to an existing warrant. Unfortunately the submission with the new telephone number included an incorrect telephone number. This resulted in the wrong telephone number being intercepted. The number was subsequently deleted from the warrant; no product was obtained and there was no interference with privacy. Security Service officers have been reminded of the importance of carrying out thorough checks of telephone numbers added to interception warrants.

2.16 The second error occurred when a target changed his mobile telephone number prior to an application being made to the Home Office for a warrant but the Security Service submitted his old number for inclusion on the warrant. The warrant with this wrong number was duly signed by the Home Secretary. The interception was suspended immediately the oversight was identified. No communications had been intercepted and no product received. Security Service officers have been reminded of the importance of carrying out thorough checks of telephone numbers added to interception warrants.

2.17 The third case involved a warrant where two digits had mistakenly been transposed when the warrant was applied for resulting in an incorrect telephone number being intercepted. None of the product from the interception had been transcribed and all the product has since been destroyed. Security Service officers have been reminded to be more diligent when checking telephone numbers in future.

2.18 **HM Revenue and Customs (HMRC)** reported one error where, in light of a decision not to renew a warrant, they allowed a warrant to run up until its end date. On that date a request was made to the HMRC case officer to cancel the warrant with immediate effect which the case officer failed to do until the following day. This resulted in some calls being intercepted without a warrant in place. The warrant was duly cancelled and all intercepted material was subsequently destroyed. HMRC's internal processes have been enhanced to ensure no recurrence of a similar error in future.

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

2.20 The first error, reported by a communications service provider itself, occurred when they intercepted a wrong telephone number; the error coming to light when the receiving agency reported that they were not receiving any product. An investigation at the CSP revealed that the error arose out of a human mistake when one of the digits was recorded incorrectly. All staff at the CSP have been reminded of the need for complete accuracy and the serious consequences of simple mistakes.

2.21 The second error, reported by the Security Service, occurred when a telephone number was added to an existing warrant. Subsequent product revealed conversations unrelated to the target. No faults could be found in the Security Service's equipment or procedures but all product relating to the unrelated conversations has been destroyed. Further investigations have been undertaken to resolve the problem.

2.22 No errors were reported by the **Home Office, Foreign and Commonwealth Office, Scottish Government, Ministry of Defence, Secret Intelligence Service, Serious Organised Crime Agency and Metropolitan Police Counter Terrorism Command**.

Statistics

2.23 **Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2007 and (b) issued during the period 1 January 2007 and 31 December 2007**

	a	*b*
Home Secretary	929 [754]*	1881
The total number of RIPA modifications from 01/01/2007 – 31/12/2007 = 5577		
Scottish Executive	28 [43]*	145
The total number of RIPA modifications from 01/01/2007 – 31/12/2007 = 367		

**For comparison purposes I have included in the parentheses the warrants in force as at 31 December 2006 as detailed in my 2006 Annual Report. I have not included the number of warrants issued during 2006 as the statistics in my 2006 Report were for a shorter period i.e., my first nine months in post – the period from 1 April 2006 to 31 December 2006. No realistic comparison can therefore be made.*

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

Section 3: Part I Chapter II – Acquisition and Disclosure Communications Data

General

3.1 The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or what was written. Certain public authorities are approved by Parliament to acquire communications data and amongst others they include the intelligence agencies, police forces, local authorities and other law enforcement agencies, such as Her Majesty's Revenue & Customs. The Act and its Code of Practice contain explicit human rights safeguards – particularly to safeguard the rights of individuals to respect for their private lives. These safeguards include restrictions set by Parliament on the purposes for which public authorities may obtain data; on what data public authorities may obtain; on which senior officials within public authorities may exercise the power to obtain data; and on which individuals within public authorities undertake the work to obtain data.

3.2 All public authorities, permitted by Parliament to obtain communications data using the provisions of RIPA, are required to adhere to a Code of Practice when exercising their powers and duties under the Act. Generally the acquisition of communications data under the Act involves four roles within a public authority and these are the applicant, designated person, single point of contact and the senior responsible officer. Persons who are involved in processing and approving applications for communications data have key responsibilities under the Code of Practice and they have a duty to ensure that the public authority acts in a lawful and informed manner. Additionally, designated persons must generally be able to act objectively and independently when approving applications for communications data and they must have a current working knowledge of human rights principles, specifically those of necessity and proportionality. Good adherence to the Code of Practice is essential if the rights of individuals are to be respected and all public authorities have a requirement to report any errors which result in unlawful intrusion.

3.3 I have a responsibility to oversee the use which public authorities have made of their powers under the Act and how they have exercised their rights and responsibilities. In this respect I am supported by a Chief Inspector and five Inspectors who all have experience of managing or supporting criminal investigations and are highly trained in the field of communications data. A programme of inspections is drawn up with the assistance of members of my Secretariat and the Inspectors firstly engage with the Senior Responsible Officer (SRO) from the public authority concerned. For example, this would normally be a Superintendent in a police force or a Head of Service in a local authority.

3.4 Within every public authority each SRO must be responsible for:

- the integrity of the process to acquire communications data;
- compliance with the Code of Practice;
- oversight of the reporting of errors to me, identifying their causes and taking
- appropriate action to minimize the repetition of errors;
- engagement with my Inspectors and ensuring that all relevant records are produced for the inspection;
- oversight of the implementation of post-inspection Action Plans, approved by me.

3.5 Following each inspection a detailed report is prepared by the Inspector and this will outline *inter alia* what level of compliance has been achieved with the Code of Practice. Where necessary the Inspector will produce a schedule

of recommendations or an Action Plan which will address all areas that require remedial action. I have sight of all of those inspection reports in order that I can properly discharge my oversight functions. The top copy of the report is sent to the head of the public authority concerned, e.g., the Chief Constable or the Chief Executive in the case of a local authority and they are required to confirm, within a prescribed time period, whether the findings are accepted and that the recommendations or action points will be implemented.

3.6 I strongly believe that it is in the public interest that public authorities should demonstrate that they make lawful and effective use of regulated investigatory powers. My annual report should provide the necessary reassurance that the use which public authorities have made of their powers has met my expectations and those of my Inspectors, although there is no reason why public authorities cannot make a further disclosure in compliance with a request under the Freedom of Information Act if they so wish. There is provision for this in the Code of Practice although each public authority must seek my prior approval before making any further disclosure. That is to ensure that the wider public interest is not adversely affected by a disclosure.

3.7 During the year ended 31 December, 2007, public authorities as a whole, made 519,260 requests for communications data to Communication Service Providers (CSP). I do not intend to give a breakdown of these requests because I do not think that it would serve any useful purpose, but I can say that the intelligence agencies, police forces and other law enforcement agencies are the principal users of communications data. Later in my report I will give some indication of the extent to which local authorities use communications data as I believe that this should be placed in context. Any suggestion that a low ranking council employee may have unrestricted access to the telephone records of a member of the public is far removed from reality because a process has to be gone through first which requires the necessity and proportionality tests to be fully met before the necessary approval is given by a senior official.

3.8 In the same 12-month period a total of 1,182 errors were reported to my office by public authorities: approximately two thirds are attributable to public authorities and one third to CSPs. This may seem a large number but it is very small when it is compared to the numbers of requests for data which are made nationally. I am not convinced that any useful purpose would be served by providing a more detailed report of these errors. I should add that neither I nor any of my Inspectors have uncovered any willful or reckless conduct which has been the cause of these errors. A considerable proportion of these errors were due to the incorrect transposition of telephone numbers and of course human error can never be eliminated completely. I am pleased to say that more and more police forces are introducing automated systems for the management of communications data requests and these will inevitably reduce the number of keying errors which occur.

3.9 In October 2007, when the Code of Practice was approved by Parliament, changes were made to the arrangements under which public authorities report errors because previously they were required to notify me of any error, even though it did not result in any intrusion upon the privacy of an innocent third party. For example, if subscriber information was requested erroneously, in relation to a telephone number which did not even exist, then this would still have to be reported as an error. Additionally, certain other errors which were effectively procedural breaches of the Code of Practice, also had to be reported. For example, the failure by a police force to serve a Notice upon a CSP retrospectively within one working day of an oral request being made for communications data when there was an immediate threat to life.

3.10 Accordingly I agreed to a change in the error reporting system whereby public authorities now only report errors which have resulted in them obtaining the wrong communications data and where this has resulted in intrusion upon the privacy of an innocent third party. In my judgment this change was necessary

in order to highlight the most serious errors which have impacted, or potentially impacted upon individuals and to reduce unnecessary bureaucracy associated with reporting of procedural error, particularly in relation to the police forces and law enforcement agencies, and to bring more perspective and clarity to the error reporting system. During the period October to December 2007 the number of 'reportable' errors made by public authorities was 99 which illustrates that in reality the level of intrusion upon innocent third parties is actually much less than stated in previous reports. Nevertheless my Inspectors review these errors during the inspections to ascertain why they occurred and how recurrence can be avoided, and they work closely with the public authorities to ensure that errors are kept to the absolute minimum.

3.11 With effect from October 2007 each public authority must also keep a log of any 'recordable' errors which have occurred during the process of acquiring communications data. Generally these are procedural errors relating to non-compliance with the Code of Practice but which do not affect its lawful entitlement to acquire the data. I have already given one or two examples of these types of error in the preceding paragraphs. These errors have to be recorded and the record produced on inspections, as they are relevant to the inspection, and because the errors may also indicate underlying problems within the systems and processes for acquiring communications data which may require remedial attention. The frequency of 'recordable' errors may indicate to an Inspector that the overall level of compliance may not be quite as good as it should be and this is important.

Communications data and the work of the Inspectorate during the period covered by this Report

Police Forces and Law Enforcement Agencies

3.12 There are 43 police forces in England & Wales; eight police forces in Scotland; and the Police Service of Northern Ireland which are all subject to inspection. Additionally my inspectors also inspect the British Transport Police; Port of Liverpool Police; Port of Dover Police; Royal Military Police; Royal Air Force Police; Civil Nuclear Constabulary; Ministry of Defence Police; and the Royal Navy Police.

3.13 Law enforcement agencies comprise Her Majesty's Revenue and Customs; the Serious Organised Crime Agency; Scottish Crime and Drug Enforcement Agency and the United Kingdom Border Agency.

3.14 In 2006 my inspectors completed the first phase inspections of the above public authorities and on the whole they were satisfied that the authorities had systems and processes in place which were fit for purpose and which ensured that they were able to achieve a good level of compliance with the Code of Practice. A number of the police forces have acquired new automated systems since then or are in the process of re-developing existing ones to make them more efficient and effective and, as indicated above, this has also helped to reduce the scope for keying errors.

3.15 In 2007 my team of Inspectors commenced the Phase 2 inspection programme and during the year they conducted 33 inspections of police forces. They also inspected HMRC and SOCA for the second time. Four of the 33 inspections of police forces were re-inspections which were carried over from the first phase. The Inspectors felt there was a need for this because certain aspects of the systems and processes were not fully compliant with the Code of Practice and not, I hasten to add, because the forces concerned were doing anything unlawful. In each case the force had implemented the recommendations from the previous inspection and this had significantly improved the level of compliance.

3.16 During phase two of the inspections greater emphasis has been placed upon the use which police forces and law enforcement agencies are making of the communications data which they obtain. They have been required to demonstrate

on a case by case basis that it was necessary and proportionate to obtain the data and that it has been used for a correct statutory purpose. From these inspections it is evident that the acquisition of the data was justified and that it is being used as a powerful investigative tool, primarily to prevent crime and disorder. It is also apparent that communications data plays a crucial role in the successful outcome of prosecutions and often it is the primary reason why offenders plead guilty.

3.17 Good use is also being made of the urgent oral process to acquire communications data when there is an immediate threat to life. Usually this applies when vulnerable or suicidal persons are reported missing but the process may also be used in kidnap situations or in other crimes involving serious violence. The importance of this facility, particularly to police forces, is obvious, and the interaction between relevant staff and CSPs saves lives across the country on a daily basis.

3.18 The inspections have established that the police forces and law enforcement agencies are managing to achieve a good level of compliance with the Code of Practice. Prior to the inspections taking place my Inspectors obtain details of the communications data which has been supplied by individual CSPs. Some of this information is randomly selected for comparison against the records kept by the public authorities and in each instance the inspectors have been satisfied that the data obtained from the CSP was acquired with the necessary and appropriate approval of a designated person. Applications for communications data are vetted robustly by trained staff, accredited communications data investigators, and more and more of the police forces and law enforcement agencies are placing the responsibility for approving applications in the hands of a core number of designated persons who are not directly involved in the investigations or operations which ensures expertise and a greater degree of independence and objectivity.

3.19 Where necessary my Inspectors will challenge the justifications for acquiring communications data if they believe that it was obtained unnecessarily or inappropriately. In one instance an Assistant Chief Constable was brought in to help resolve a case of difficulty. This demonstrates the importance of the inspection process to the police forces and their willingness to comply with the inspection regime. Under the Code of Practice I have the power to direct a public authority to provide information to an individual who has been adversely affected by any wilful or reckless exercise or lack of exercise of its powers under the Act. So far it has not been necessary for me to exercise this function but there is no room for complacency and each police force and law enforcement agency understands that it must strive to achieve the highest possible standards. In my view the inspection programme encourages this.

3.20 A key aim of inspections has been to make recommendations which are designed to sweep away unnecessary bureaucracy from the systems and processes whilst still ensuring that there is full accountability in the acquisition of the data. Often valuable police time and resources could be saved if some of the processes were streamlined through the use of fewer forms, or by the use of documents which are produced in a better and more simplified format. It is disappointing that some police forces have been slow to take up these recommendations but my inspectors will keep on urging them to do so, as it will enable relevant staff to free up more of their time to concentrate upon quality assurance and raising standards across the board.

Security and intelligence agencies

3.21 For the most part the work of the intelligence agencies is necessarily secret and therefore this limits what I can say about the inspections which have been conducted in relation to their use of data. However, I can state that the intelligence agencies are subject to exactly the same type of inspection as police forces and law enforcement agencies. I am satisfied that they are complying with the Act and Code of Practice and no issues have arisen regarding their application of the legislation.

3.22 Communications data is used extensively by the intelligence agencies, primarily to build up an intelligence picture about persons or groups of persons who may pose a real threat to our national security. Given the nature of the work it is perhaps unavoidable that there will be some degree of collateral intrusion into the private lives of persons who have had contact with the subjects of investigations. However, this is recognised by the intelligence agencies, and the inspections have shown that intrusion is being limited so far as possible.

Local Authorities

3.23 There are approximately 474 local authorities throughout the UK approved by Parliament for the purpose of acquiring communications data, using the provisions of the Act. No local authority has been given the power to intercept a telephone call or any other form of communication during the course of its transmission. Local authorities may acquire communications data for the purpose of preventing and detecting crime, but there are restrictions upon the types of data which they may obtain. They do not have access to traffic data which would enable them to identify the location from or to which a communication has been transmitted.

3.24 Generally the trading standards services are the principal users of communications data within local authorities although the environmental health departments and housing benefit fraud investigators also occasionally make use of the powers. Local authorities enforce numerous statutes and Councils use communications data to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. The environmental health departments principally use communications data to identify fly-tippers whose activities cause damage to the environment and cost the taxpayers large sums to recover or otherwise deal with the waste.

3.25 Local authorities are required to adhere to the Code of Practice and requests for communications data are approved at a senior level. In most cases this will be the head of the trading standards service or the heads of the environmental health departments or housing benefits sections although solicitors are also often involved. The specialist staff, who process applications for communications data, are not trained to the same standard as their counterparts in other public authorities and this has caused difficulties for some local authorities, which have not been able to attain the best possible level of compliance with the Code of Practice.

3.26 During the period covered by this report only 154 local authorities made use of their powers to acquire communications data. A total of 1,707 requests were made for communications data and the vast majority were for basic subscriber information. Very few local authorities have used their powers to acquire itemized call records in relation to the investigations which they have conducted. Indeed our inspections have shown that generally the local authorities could make much more use of communications data as a powerful tool to investigate crime.

3.27 Virtually all of the local authorities which have used their powers have been inspected at least once during the last two years. Last year inspections were carried out at 44 local authorities and this included two re-inspections, which were necessary because the level of compliance was not as good as it should have been.

3.28 Quite a number of local authorities have struggled to achieve the best possible level of compliance with the Act and Code of Practice. This is largely because they make very infrequent use of their powers and consequently the staff who process and approve applications for communications data are often not familiar with all aspects of the Code of Practice. Additionally the training which they received when the legislation was introduced in 2004 was very basic and there has been little or no provision made for them to up-skill themselves. Consequently my inspectors find that they spend a great deal of time re-educating the staff and helping them modernise the system and processes. The local authorities have responded positively and rarely, if ever, do they fail to accept the findings of the inspection or implement the action points and recommendations. I would

recommend that the Home Office considers reviewing the provision of training to ensure that it is practical and supports the single points of contact and designated officers in their work.

3.29 The local authorities reported a total of 52 errors in 2007 and a fair proportion of these were identified during the inspections. In the main these errors have been caused through failure to comply with technical aspects of the Act or Code of Practice. In some cases the data was not obtained fully in accordance with the law because, for example, the Notice was not given by the designated person before it was served upon the CSP. However, in the vast majority of these instances the Inspector was satisfied that the acquisition of the data was justified, and that it could have been acquired lawfully if the proper procedures had been followed. I have not encountered any cases which would be serious enough for me to invoke the powers which I have outlined previously in paragraph 3.19 of this report.

3.30 Bearing in mind the difficulties which some local authorities have experienced and the considerable costs, which are involved in training staff and maintaining systems and processes, I suggested to the Home Office that better arrangements should be made for the acquisition of communications data by local authorities. This has been acted upon and currently the Home Office is conducting a scoping exercise with the National Anti-Fraud Network (NAFN) to see whether it could provide a national service for its member local authorities. The exact details have still to be ironed out but it is envisaged that local authorities will be able to submit approved applications to NAFN which will then undertake the process of retrieving the data from the CSPs. Suitable staff from NAFN will be trained by the Data Communications Group, which trains police SPoCs at the West Mercia Constabulary so that they will have the appropriate skills and accreditation to process these applications. This facility should help local authorities, which opt into the scheme, to achieve the best possible level of compliance with the Code of Practice.

Other public authorities

3.31 There are approximately 110 other public authorities which are registered for the purpose of acquiring communications data. These include the Serious Fraud Office, Independent Police Complaints Commission, Charity Commission, Royal Mail and the Medicines & Healthcare Products Regulatory Agency (MHPRA) to name just a few.

3.32 It has not been possible to inspect every one of these public authorities during the period covered by this report although they have all been inspected at least once during the last two years. Many of these public authorities make very limited use of their powers and only acquire communications data for specialist purposes. For example, MHPRA investigates alleged breaches of the medicines and medical devices legislation for which the penalty may be imprisonment or a significant fine. Communications data is used to investigate these offences and this is a necessary tool to combat the growing threat of Internet sales of unlicensed and non-compliant products.

3.33 The inspections established that in almost every case these public authorities are using their powers responsibly and that the communications data is being acquired for a correct statutory purpose. They also have a requirement to comply with the Code of Practice and this is borne out from the inspections. In all cases the findings of the inspection reports have been accepted and the vast majority of the recommendations have been implemented.

Section 4: Interception in Prisons

General

4.1 At the request of the Secretary of State I have continued to provide the oversight of the interception of communications in prisons in England & Wales. This is a non-statutory role and in practice most of the inspections are conducted by my Inspectors although I have sight of every report which they produce.

4.2 The interception of prisoners' telephone calls and correspondence is permitted, and in many cases is mandatory, under the Prison Act 1952 and the National Security Framework (NSF). The NSF stipulates that any telephone call may be listened to or letter read if intelligence suggests that this is necessary and proportionate under Prison Rule 35A or Young Offenders Institution Rule (YOIR) 11(4). Interception is mandatory, primarily in the case of Category A prisoners and prisoners who have been convicted of sexual or harassment offences and who continue to pose a risk to children or the public. However, communications which are subject to legal privilege are protected and there are also special arrangements in place for dealing with confidential matters, such as contact with the Samaritans and a prisoner's constituency MP.

Work of the Inspectorate during the period covered by this Report

4.3 There are 137 prisons in England & Wales, including Kennet which was opened in 2007. All of the prisons have been inspected on at least one occasion during the last 3 years and quite a number have now been inspected for a second or third time. During the period covered by this report my Inspectors visited 85 prisons which roughly equates to two thirds of the whole estate. The inspection usually takes one working day although in order to achieve this in the larger prisons the Inspectors work in pairs. Following the conclusion of the inspection a detailed report is prepared for me and this is sent to the Governor and relevant staff, together with a schedule of recommendations or an Action Plan if necessary.

4.4 There is a legal obligation upon the Prison Service to inform the prisoners, verbally and in writing, that their communications are subject to interception. Interception is illegal and a breach of the Human Rights Act unless it is carried out in accordance with the Act and NSF. The primary objective of the inspection is to ensure that each prison is complying with the rules.

4.5 Regrettably, I cannot give an assurance that there is total compliance with the rules and in some prisons breaches still occur on a fairly regular basis. My inspectors have needed to re-inspect a number of prisons within a relatively short time in order to raise the level of compliance. In saying so, however, I do not imply that prison managers and their staff are deliberately setting out to circumvent the rules. Generally failure to achieve a good level of compliance results from a lack of resources and the pressure which the staff are often under to deal with other matters involving the good order and security of the prison.

4.6 Towards the end of last year my Chief Inspector and I met with the Director General of the Prison Service to review the outcomes from the various inspections and this was very useful. A new strategy for conducting the interception of communications within prisons has now been developed by the National Intelligence Unit and this is based upon the findings from the inspections. The intention is that the new scheme will be tried in a number of prisons which have been selected by the Prison Service and then the results and findings will be presented to the Secretary of State for consideration.

4.7 Gradually, the level of compliance is improving and indeed some prisons have exceeded all expectations. A new document, which contains all of the salient features of the interception of communications, has been developed and this is being adopted universally. Signed acknowledgements are to be obtained from each prisoner and retained in the core records as this will clearly demonstrate that the prison has fully discharged its legal obligations.

4.8 I am reasonably confident that in time our inspections will show that there is general compliance with the Act and the Rules which are laid down under it. Without fail the Governors are responding very positively to our recommendations and in my view the new strategy will ensure that in the longer term there will be improved efficiency and effectiveness.

Section 5: Other Matters

Foreign and Commonwealth Office and Northern Ireland Office warrants

5.1 In paragraphs 31 – 33 of my Annual Report for 2006, I 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.

5.2 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."*

5.3 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 paragraph 2.* of 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.

Safeguards

5.4 Sections 15 and 16 of RIPA lay a duty on the Secretary of State to ensure that arrangements are in force as safeguards in relation to the dissemination, disclosing, copying, storage and destruction etc., of intercepted material. These sections of the legislation require careful and detailed safeguards to be drafted by each of the agencies and for those safeguards to be approved by the Secretary of State. This has been done. My advice is sought on proposed amendments to the safeguards when they are updated in light of technical and administrative developments. During the period of this report I saw and commented on the revised handling arrangements for the Police Service of Northern Ireland and the Serious Organised Crime Agency. I also assured officials in HM Revenue and Customs (HMRC) that I was satisfied with the adequacy of the safeguards they had in place to deal with disclosure following adverse criticism of an HMRC officer by a Court of Appeal judge.

House of Commons' Joint Committee on Human Rights: Intercept as Evidence

5.5 In paragraph 61 of my first Annual Report last year, I referred briefly to the debate about whether or not intercept product should be used as evidence in a court of law. Though I was not called to give evidence myself before the House

of Commons' Joint Committee on Human Rights I think it is right to record that my predecessor as Interception of Communications Commissioner – Sir Swinton Thomas – did give oral evidence to that Committee in public on 12 March 2007 on whether or not to relax the ban on the admissibility of intercept evidence. Whilst Sir Swinton Thomas and I share the same view that the benefits of any change in the law are heavily outweighed by the disadvantages, I do not intend rehearsing here the arguments that Sir Swinton Thomas addressed to the Committee. These have been reflected in the Committee's Nineteenth Report of the 2006-2007 Session published on 30 July 2007 (HL Paper 157, HC 394).

Section 6: The Investigatory Powers Tribunal

Statistics

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

6.2 As I explained in paragraph 39 of my Annual Report for 2006, complaints to the Investigatory Powers 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 previously have 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 66 new applications during the calendar year 1 January 2007 – 31 December 2007 and completed its investigation of 31 of these during the year as well as concluding its investigation of 52 of the cases carried over from 2007. 41 cases have been carried forward to 2008.

Assistance to the Tribunal

6.3 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. During 2007 I was asked by the Tribunal President to assist the Tribunal on one occasion. The legislation precludes me from identifying details of the particular complaint but for the purposes of this Report I can say that I provided advice to the President as to whether the test of "necessity" was correctly applied when an agency was considering whether or not it was "necessary" for a particular person's telephone calls to be intercepted "for the purpose of preventing or detecting serious crime".

Section 7: Conclusion

7.1 As I said in my first Report last year, the interception of communications is an invaluable weapon for the purposes set out in section 5(3) of RIPA. It has continued to play a vital part in the battle against terrorism and serious crime, and one that would not have been achieved by other means. The task of the agencies working in this field has become, and is becoming ever more, technical and difficult as a result of the greater sophistication of terrorists and criminals. I am satisfied that Ministers and the intelligence and law enforcement agencies carry out the work which I am required to consider diligently and in accordance with the law.

7.2 I said last year that in times like these the Wilson Doctrine seems to me to be indefensible. That is still my belief, and, judging by the reaction to a complaint made by a Member of Parliament some months ago, it is a belief that is widely shared.

7.3 I also said last year, and I repeat, that my work would be impossible without the generous support of the small secretariat which works with me, with the Intelligence Services Commissioner, and with the Investigatory Powers Tribunal. They, and the inspectors to whom I have referred, have all done excellent work, and I am very grateful to them.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
07/08 405169 19585

Printed on Paper containing 75% recycled fibre content minimum.

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

Online
www.tsoshop.co.uk

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

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX

TSO@Blackwell and other Accredited Agents