# Report of the Interception of Communications Commissioner for 2009

Commissioner:
THE RT HON SIR PAUL KENNEDY

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

Ordered by the House of Commons
to be printed
27 July 2010

Laid before the Scottish Parliament by
the Scottish Ministers
July 2010

HC 341
SG/2010/135

£5.75

# Report of the Interception of Communications Commissioner for 2009

Commissioner:
THE RT HON SIR PAUL KENNEDY

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

Ordered by the House of Commons to be printed
27 July 2010

Laid before the Scottish Parliament by the Scottish Ministers
July 2010

HC 341
SG/2010/135

£5.75

ISBN: 9780102968422

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2379339 07/10 4458 19585

Printed on paper containing 75% recycled fibre content minimum.

# Contents

From: The Right Honourable Sir Paul Kennedy

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

22 June 2010

I enclose my fourth Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. The Report covers the period 1 January 2009 to 31 December 2009. It is, of course, for you to decide, after consultation with me, how much of the report should be excluded from publication on the grounds that it is prejudicial to national security, to the prevention or detection of serious crime, to the economic well-being of the United Kingdom, or to 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the course of writing the report in two parts, the Confidential Annex containing those matters which in my view should not be published.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. David Cameron MP
10 Downing Street
London SW1A 2AA

# Annual Report of the Interception of Communications Commissioner for 2009

## 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 was initially for three years and has, since 11 April 2009, been extended for a further period of three years to 10 April 2012.

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 fourth annual report as Commissioner and it covers the period 1 January 2009 until 31 December 2009. 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 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 (the acquisition and disclosure of communications data);

(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 (investigation of electronic data protected by encryption etc); 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.

1.5 As Commissioner, it is also my function 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 it to carry out its functions under that section.

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 Chapter 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 of Northern Ireland, the Northern Ireland Office, HM Revenue and Customs, the Foreign and Commonwealth Office, the Home Office, the Scottish Government 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. These include both warrants and attendant certificates. 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 continue to be impressed by the quality, dedication and enthusiasm of the personnel carrying out this work. They possess a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards. All applications made to the Secretary of State are scrutinised by officials in the warrants unit within their respective Departments (e.g., the Home Office, the Foreign Office and the Ministry of Defence and by similar officers in departments in the Northern Ireland Office and Scottish Government). 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 the personnel and documents that I have asked to see. They welcome my oversight, as ensuring that they are acting lawfully, proportionately and appropriately, and they seek my advice whenever it is deemed appropriate. 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, the Secretary of State for Northern Ireland and the Scottish Government Cabinet Secretary for Justice. It is clear to me that each of them gives a substantial amount of time and takes considerable care to satisfy himself or herself that the warrants are necessary for the authorised purposes, and that what is proposed is proportionate. If the Secretary of State wishes to have further information in order to be satisfied that he or she should grant the warrant then it is requested and given. Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity 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 2009, I visited a total of nine 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 intercepting agencies. Those in the CSPs and ISPs who work in this field are committed and professional. They recognise the importance of 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 meeting of the Intelligence and Security Committee on 21 April 2009 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 over the last year and the challenges ahead, changes in number of warrants and authorisations, trends in the number of interception warrant breaches and errors and the admissibility of intercept as evidence, about which I will say more later in this Report.

*Privy Council Review of Intercept as Evidence*

2.6 In paragraphs 2.6 – 2.7 of my Annual Reports for both 2007 and 2008 I reported on the Prime Minister's announcement of a Privy Council Review of Intercept as Evidence under the chairmanship of Sir John Chilcot. I think it appropriate for the sake of continuity to re-state the background to this issue again before reporting on progress.

2.7 In my Reports I commented on 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.

2.8 Since the Prime Minister's statement a lot of work has been done, led by the Home Office, 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. During 2008 I attended a number of meetings at the Home Office where I was fully briefed on the development of models 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. Operational live testing of these models took place in March and April 2009 followed by court role plays during May 2009. I saw much of the role play. In my Annual Report for 2008 (submitted in July 2009) I said that I felt that these tests highlighted real legal and operational difficulties inherent in using intercept as evidence within the UK and that I could not see a way to overcome these.

2.9 On 10 December 2009 the Home Secretary published a Report of the Privy Council's findings and conclusions. They recognised the potential gains from a workable scheme for intercept as evidence and that, while requiring significant additional funding, the model developed would be broadly consistent with the operational requirements identified. However, the Home Secretary also conceded that the model would not be legally viable, in terms of ensuring continued fairness at trial. The result would not only be potential miscarriages of justice and more expensive and complex trials, but also more of the guilty walking free.

2.10 Both the Advisory Group of Privy Counsellors and the government believe that the potential gains from intercept as evidence justify further work in order to establish whether the problems identified are capable of being resolved. The issues involved are complex and difficult. I hope to be able to report on the progress made on the planned further work in my 2010 Annual Report.

*ECHR decision: Liberty v. UK*

2.11 In paragraph 2.13 of my Annual Report for 2008 I highlighted the fact that in July 2008 the European Court of Human Rights handed down judgment in Liberty v. UK. The complaint was about interception of communications, allegedly contrary to Article 8 of the Convention. The challenge related to the way in which external interception was conducted under the previous legislation, the Interception of Communications Act 1985 (IOCA). IOCA was replaced by the Regulation of Investigatory Powers Act 2000 (RIPA) which was introduced to take proper account of human rights and which contains additional foreseeability requirements. The Home Office confirmed that they were considering whether any additional measures were required in light of the Strasbourg judgment, i.e., whether RIPA and the existing interception Code of Practice rectify legal deficiencies identified by the European Court of Human Rights.

2.12 Whilst the Home Office believes that the issues raised in the Liberty case have, to a large extent, already been addressed by the implementation of RIPA and the Code, it has decided to make some changes. Following receipt of legal advice it intends making a small number of amendments to the Code: chapter 5 (covering RIPA section 8(4) interception warrants) and chapter 6 (safeguards). These deal with how, post-interception, material gathered under warrant comes to be examined, including giving a better indication of the filtering of extraneous material via automated systems. The proposed revised draft Code of Practice was issued by the Home Office for consultation on 12 March 2010 with a deadline for responses of 7 June 2010.

*Hong Kong Independent Commission Against Corruption*

2.13 In September 2009 I met the Hong Kong Commissioner and his team of officials who were visiting the UK to examine various issues relating to the interception of communications. The meeting focussed on how the United Kingdom legislation works in practice, the methods of oversight and accountability, and compliance with the Human Rights Act. Whilst there were minor differences in the approach to interception and the gathering of intelligence between the UK

and Hong Kong, the laws and basic principles that govern such practices are the same. The discussion I had with the officers provided an interesting insight into differences in procedures and practices.

## Successes

2.14 It is impressive to see how interception has contributed to a number of striking law enforcement and national security successes during 2009. 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

2.15 Thirty six errors and breaches have been reported to me during the course of 2009. This is a 28% decrease from the total of 50 errors and breaches reported in my last Annual Report. By way of example, details of some of these errors are recorded below. It is important from the point of view of the public that I stress that none of the breaches or errors was 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. Where breaches or errors occur, procedures are subsequently revised or strengthened in order to minimise the chances of a similar mistake being made again. The most common cause of error tends to be the simple transposition of numbers by mistake e.g., 1969 instead of 1996. The examples that I give are typical of the whole 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.

2.16 Eleven errors were reported to me by **GCHQ**. By way of example, three of these errors, which were similar in nature, resulted from the failure on the part of the relevant reporting areas to ensure that decisions to remove targets from the appropriate warrantry certificate were followed up with the appropriate actions to de-activate the targeting. All items collected as a result of these failures were deleted from GCHQ's systems, and the relevant staff were reminded of the importance of the formal procedures for removing targets from or adding targets to a certificate. Extra checks have also been incorporated into the processes to prevent future recurrences.

2.17 The **Security Service** reported ten errors that were directly attributable to them. Brief details of three of these are given below.

2.18 In the first case material that was subject to journalistic privilege was not handled in accordance with the agreed procedures. This material has now been reviewed according to the established procedures and, where appropriate, has been labelled with additional caveats concerning further dissemination. The relevant investigator has been reminded of the importance of informing transcribers when targets are or may be involved in exchanges that may produce confidential material.

2.19 The second error involved a warrant where an incorrect digit was used when the warrant was applied for resulting in an incorrect telephone number being intercepted. The interception was immediately cancelled and all product destroyed.

2.20 The third error involved the failure of a desk officer to process the relevant paperwork to cancel an intercept before the warrant's expiry date. A period of 12 hours unauthorised interception ensued during which time the user of the telephone made seven outgoing calls. None of these calls were monitored and all the product has been deleted.

2.21. **HM Revenue and Customs (HMRC)** reported two errors. One of them concerned a modification for a communication address which was applied for and authorised. The application was based on information provided by a reliable covert human intelligence source (CHIS). However, when the product was received it did not seem to be relevant. Checks by HMRC established that the information provided by the CHIS was incorrect. Interception was stopped immediately. HMRC's internal vetting processes have now been enhanced to prevent similar recurrences in future.

2.22 The **Serious Organised Crime Agency (SOCA)** reported eight errors, two of which I detail below.

2.23 The first error involved a warrant where an incorrect number was used when the warrant was applied for, resulting in an incorrect telephone number being intercepted. The interception was immediately cancelled and all product destroyed. The case officer was reminded of his responsibility for checking and verifying the appropriate telephone numbers prior to submitting applications for interception.

2.24 The second error involved a warrant where two digits in a telephone number had mistakenly been transposed before the application was submitted for a warrant. This resulted in an incorrect telephone number being intercepted. The interception was cancelled and deleted from the warrant and all the product destroyed.

2.25 The **Scottish Government** reported one error in respect of an interception warrant. An application was made to intercept four telephone numbers but it transpired that when it was signed, the application only contained three telephone numbers. The warrantry paperwork is normally double-checked against the signed applications; unfortunately the draft application had been referred to when starting to intercept, so the fourth number was intercepted. Interception of the fourth line was suspended as soon as the error came to light, no product having been received. The relevant staff were reminded of the formal procedures.

2.26 The **Metropolitan Police Counter Terrorism Command** reported one error where a warrant was obtained with an incorrect email address. The warrant was cancelled and all material relating to the communications address was destroyed. Arrangements were made for future applications to be subjected to closer scrutiny.

2.27 Three errors attributable to the **National Technical Assistance Centre (NTAC)** were reported during the period of this report, one of which I now explain. NTAC reported a technical fault within their infrastructure that resulted in the prevention of delivery of intercept related information to the intercepting agencies for three days. A project to prevent this type of error occurring has been initiated and is expected to deliver improvements in the system in 2010.

2.28 No errors were reported by the **Home Office, Northern Ireland Office/ Police Service of Northern Ireland, Ministry of Defence, the Secret Intelligence Service** or any of the **communications service providers**.

## Statistics

2.29 **Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2009 and (b) issued during the period 1 January 2009 to 31 December 2009**

| | a | b |
|---|---|---|
| Home Secretary | 959 [844]* | 1514 [1508]* |
| The total number of RIPA modifications from 01/01/2009 – 31/12/2009 = 5267 [5344]* | | |
| Scottish Government | 69 [43]* | 192 [204]* |
| The total number of RIPA modifications from 01/01/2009 – 31/12/2009 = 629 [610]* | | |

* For comparison purposes I have included in the parentheses warrant information for the period 1 January 2008 to 31 December 2008 as detailed in my 2008 Annual Report.

# Section 3: Part I Chapter II – Acquisition and Disclosure of 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 to assist them in carrying out their investigatory or intelligence function and they include the intelligence agencies, police forces, Her Majesty's Revenue and Customs, the Serious Organised Crime Agency and other enforcement agencies, such as the Serious Fraud Office and Information Commissioner's Office. Local authorities, including the Trading Standards Service, are also able to acquire a restricted set of communications data to assist them to investigate complaints made by the public.

3.2 The Act and its Code of Practice contain explicit human rights safeguards-particularly the rights of individuals to have respect for their private life and correspondence. The safeguards include restrictions, prescribed by Parliament on the statutory purposes for which public authorities may obtain data; on the type of data public authorities may obtain; which senior officials within public authorities may exercise the power to obtain data; and which individuals within public authorities undertake the work to obtain data.

3.3 All public authorities, permitted to obtain communications data using the provisions of RIPA, are required to adhere to the 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, the Designated Person able to authorise applications, the Single Point of Contact (SPoC) and the Senior Responsible Officer (SRO). SPoCs are responsible for the development and processing of applications for communications data. They have key responsibilities under the Code of Practice and they also have a duty to ensure that the public authority acts in a lawful and informed manner. Additionally, Designated Persons must be able to act objectively and independently when approving applications for communications data and have a current working knowledge of human rights principles, specifically those of necessity and proportionality. Adherence to the Code of Practice by public authorities and Communications Service Providers (CSP) 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 data being disclosed.

3.4 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. Although I retain sole oversight of anything to do with interception, in relation to communications data I am supported by a Chief Inspector and five Inspectors who are all highly trained in the acquisition and disclosure processes, and in the extent to which communications data may assist public authorities in carrying out their functions. A programme of inspections is drawn up with the assistance of members of my Secretariat and the Inspectors initially engage with the SRO from the public authority concerned. For example, in a police force this must be at least a Superintendent or a Head of Service in a local authority.

3.5 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 minimise 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.

3.6 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.

3.7 I 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.

3.8 During the year ended 31 December, 2009, public authorities as a whole, made 525,130 requests for communications data to Communication Service Providers and Internet Service Providers. I do not intend to give a breakdown of the requests because I do not think that it would serve any useful purpose, although the intelligence agencies, police forces and other law enforcement agencies are the principal users of communications data. This figure is above the number of requests which were made in the previous year (504,073) and this is because certain police forces have increased their demands for communications data. I cannot give a precise reason for this but there is evidence that more and more police forces have to investigate Internet related crime, including paedophile rings and the requirements to obtain communications data in these types of cases can be quite extensive. In other words one police investigation can generate a large number of requests for 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 which requires the necessity and proportionality tests to be met before the necessary approval is given by a senior official.

3.9 In the same 12-month period a total of 661 errors were reported to my office by public authorities; approximately three quarters are attributable to public authorities and the remainder to CSPs and ISPs. 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 wilful 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 more and more police forces continue to introduce automated systems to manage their requirements for communications data and these will reduce the number of keying errors which occur.

3.10 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.

3.11 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. Other errors are simply recorded. In my judgement 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 errors, particularly in relation to the police forces and law enforcement agencies, and to bring more perspective and clarity to the error reporting system. My Inspectors review all 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. 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; 8 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; the Scottish Crime and Drug Enforcement Agency; United Kingdom Border Agency; and the Child Exploitation & Online Protection Centre.

3.14 All of the above mentioned public authorities, with the exception of the Civil Nuclear Constabulary, Port of Dover Police and the Child Exploitation & Online Protection Centre have now been inspected at least twice since the Inspectorate was formed about five years ago. The Port of Dover Police and the Port of Liverpool Police did not make any use of their powers during the reporting year and the Civil Nuclear Constabulary has made only 15 requests for communications data. The vast majority of them were for subscriber information and therefore it has not been necessary for us to conduct a second inspection.

3.15 The Child Exploitation & Online Protection Centre was formed in 2006 and it is dedicated to eradicating the sexual abuse of children. It was inspected for the first time in August last year and clearly communications data plays a key role in helping the Child Exploitation & Online Protection Centre work in partnership with local and international forces and Internet Service Providers (ISP) to make the Internet a safer place for our children and young people to use.

3.16 In 2009 my team of Inspectors commenced the third phase inspections of police forces and law enforcement agencies. Thirty three inspections of police forces and law enforcement agencies were conducted during the reporting year. The areas covered by these inspections are fairly wide ranging and therefore the Inspectors work in pairs because experience shows this is more efficient and effective. Later in this section of this report I intend to give more insight into how the inspections are conducted because I believe this will give the necessary reassurance that relevant public authorities are held accountable for the way in which they exercise their powers to acquire communications data.

3.17 Generally the outcomes of the inspections were good and the Inspectors concluded that communications data is being obtained lawfully and for a correct statutory purpose. One of the first aims of the inspection is to check that the recommendations or action points from the previous inspection have been implemented and this proved to be so in the vast majority of cases. As a consequence the overwhelming number of police forces and law enforcement agencies are sustaining a good level of compliance with the Act and Code of Practice. However, it came to my notice that one or two police forces had been slow to respond to the findings from the previous inspection reports. They were revisited a few months later and the necessary improvements had been made.

3.18 I am pleased to report that a considerable number of police forces and law enforcement agencies have automated systems for the purpose of managing their requirements for communications data, and they are continually being upgraded to ensure they work as efficiently and effectively as possible. They help to reduce the scope for errors as generally the subject telephone number or communications address only has to be entered once and then it populates itself throughout the remainder of the process. In one instance, however, minor breaches of the Act and Code of Practice were occurring because the software had been modified inappropriately after it had been installed. In effect this meant that some of the data had not been obtained fully in accordance with the law and relevant staff in the public authority concerned have been advised that they have a duty under the Criminal Procedure and Investigations Act 1996 to bring this to the attention of the prosecutor who will decide whether it could have an adverse effect on any criminal proceedings which are pending. In my view this is improbable because the Inspectors were satisfied that it was still necessary and proportionate to acquire the data and moreover it could easily have been obtained lawfully if these procedural breaches had not occurred. Where necessary my Inspectors have liaised with the systems providers to make sure that the automated systems are capable of operating fully within the law and the Code of Practice.

3.19 Part of the inspection entails checking whether the systems and processes for acquiring communications data are being maintained efficiently and effectively. Inherent failings and weaknesses must be identified and quickly remedied in order to minimise the risk of errors. Generally the police forces and law enforcement

agencies emerged well from this aspect of the inspection although it is important that they have the right number of well trained staff in this business area. It was disappointing to find that almost half of the police forces inspected had taken little or no advantage of certain streamlining procedures which were introduced when the Code of Practice was approved by Parliament in October 2007. The changes were introduced to eliminate unnecessary bureaucracy and to make sure valuable police time is not wasted. When necessary these matters are drawn to the attention of the Chief Constables in a covering letter which is issued with each inspection report. The responses have all been positive and system changes have generally now been implemented to increase efficiency and effectiveness.

3.20 My Inspectorate receives good cooperation from the CSPs who have a requirement to comply with any lawful requests for communications data which are received from the public authorities. Once again the CSPs were asked to provide my Inspectors with details of the communications data they had disclosed to the public authorities during a specified period. These disclosures were randomly checked against the records kept by the public authorities in order to verify that documentation was available to support the acquisition of the data. I am pleased to say that in all cases my Inspectors were satisfied the correct process had been applied and the data had been obtained with the approval of a designated person. I regard this as a very important check upon the integrity of the process and it is most reassuring that so far it has not exposed any instances of abuse or the unlawful acquisition of communications data.

3.21 As in the previous year a great deal of emphasis has been placed upon the use which police forces and law enforcement agencies are making of the communications data which they have obtained from CSPs. 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. My Inspectors are able to assess this in two different ways and when necessary they have challenged the justifications for acquiring a specific set of data.

3.22 First, they have carried out a random examination of applications from various sectors of the business in order to judge the overall standard of the public authority. The accredited officers in the Single Point of Contact have a responsibility under the Code of Practice to make sure the public authority acts in a lawful and informed manner and therefore they should return any applications which do not meet the required standard. All of the police forces and law enforcement agencies which were inspected during the reporting year achieved a satisfactory standard and indeed 80% of them were consistently producing good quality applications.

3.23 Secondly, in each police force or law enforcement agency the Inspectors will look in detail at two or three operations, normally where communications data has been used to investigate major incidents or serious crime. They will examine a number of the applications and conduct informal interviews with senior investigating officers, applicants and analysts. If necessary they will, and often do, challenge the justifications for acquiring the data. The results of this part of the inspection have been very revealing and generally it is evident that good use has been made of the communications data as a powerful investigative tool, primarily to prevent and detect crime and disorder. It is also very 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.

3.24 I would like to give a few examples of how communications data is used by police forces and law enforcement agencies to investigate criminal offences. It may provide a better understanding of its importance to a criminal investigation and the following examples are based on extracts from the Inspector's reports. For obvious reasons I do not intend to reveal the strategies for using communications data as that may inhibit the conduct of future investigations.

3.25 In the first case Lothian and Borders Police commenced an investigation when indecent images of child abuse were found on the hard drive of a computer which was sent in for repair. The owner of the computer, Neil Strachan, was a registered sex offender and he was arrested. The computer was forensically examined and evidence was found to show that Strachan was a principal member of a paedophile ring which was manufacturing and distributing indecent images of children on a huge scale. The use of communications data was vital during the course of this investigation because it helped the police to identify and trace a large number of his accomplices and bring them to justice. In October 2009 Neil Strachan and James Rennie both received life sentences and six other members of the paedophile ring, which was by far the largest ever encountered in Scotland, were jailed for approximately 43 years.

3.26 The second case also involved a paedophile ring which was based mainly in the Northeast of England and North Wales but it has since been established that indecent images of children have been sent to all corners of the UK. This group of individuals was detected purely by chance when one of them mistakenly left a mobile telephone on a bus in Newcastle City Centre. A member of the public handed it in to Northumbria Police who initially examined it with the intention of returning it to the owner and then the investigation was launched when it was found to contain indecent material. It led them to a succession of other men, who themselves had been sharing indecent material with fellow paedophiles, using other handsets and computers, creating a UK-wide web of depravity. So far 21 arrests have been made and approximately 100 packages of intelligence and evidence have been sent to Forces nationwide. The acquisition of communications data was central to this investigation and the original offender received an indeterminate sentence when he appeared at Newcastle Crown Court in December 2009. He will have to serve a minimum of 5 years before he can be considered for release.

3.27 Distraction burglary is where a bogus caller tells lies to gain entry into a home or creates a diversion so that an accomplice can sneak in and steal property. The perpetrators generally target the vulnerable and the elderly and often they pose as officials from the water board, gas company or even police officers to gain access to private houses. Once inside they will often use violence or intimidation to force the householders to part with their possessions. Hampshire Constabulary investigated three men who were responsible for over 70 distraction burglary offences in Hampshire and other parts of the UK. The weight of the communications data was a key factor in the offenders deciding to plead guilty. In June 2009 they each received a sentence of 10 years imprisonment. In passing sentence the Judge remarked that the three defendants had planned the offences in a professional and calculated way and it was as bad a series of burglaries as had ever been before him.

3.28 Drug trafficking organisations use mobile telephones and other communications devices to conduct their criminal activities. One of the key aims of the investigators is to attribute these devices to the individual members of the drug trafficking group so that communications data can then be adduced in evidence to help prove that they were conspiring with each other to commit criminal offences. Invariably analytical charts are produced to show the location of the communications devices throughout the period of the conspiracy and in this way defendants can be linked with the key events, such as the importation or distribution of quantities of controlled drugs. Suffolk Constabulary used this to very good effect when intelligence indicated that an individual who had no visible means of income had acquired vast wealth from drug trafficking. Ultimately 16 persons were charged with drug trafficking and they all pleaded guilty. The seven principal defendants received sentences totalling 32 years. Street cash and assets to the value of £750,000 have been seized together with quantities of Class A drugs.

3.29 Police SPoCs throughout the UK provide a very valuable service to the staff who carry out these investigations and often they make a significant contribution

to the successful outcome of casework. Despite the above successes it is perhaps inevitable that some mistakes will be made, especially when public authorities are dealing with large volumes of communications data in complex investigations. Overall the error rate is low and indeed minute when compared to the huge number of requests which were received by the CSPs during the course of the reporting year.

3.30 The urgent oral process should only be used when a person's life might be endangered if the application procedure were to be undertaken in writing from the outset, or when an opportunity to make arrests, or seize illicit material may be lost. It is also accepted that police forces will need to use the urgent oral process when dealing with sudden deaths, serious injuries and vulnerable persons if undertaking the application process in writing from the outset would cause unnecessary suffering and trauma to the next of kin.

3.31 Good use is being made of the urgent oral process to acquire communications data when there are immediate threats to life. Usually this applies when vulnerable or suicidal persons are reported missing but the process is also used in kidnap situations or in other crimes involving serious violence. During a six month period the 33 police forces and law enforcement agencies which were inspected last year used the urgent oral process on approximately 8,245 occasions. Mainly it was used in connection with enquiries involving immediate threats to life. This is an important facility, particularly for police forces, and the interaction between relevant police staff and CSPs saves lives across the country on a continuous basis. Marked improvements were found in the management of the process and the quality of the record-keeping in comparison with previous years. There is no obvious explanation for the large increase in resort to the urgent oral process as compared with last year. The recommendations from the previous inspections were implemented and as a consequence better standards are being achieved.

3.32 It is estimated that well over 80% of the requests for communications data are for subscriber information and they can only be approved by an Inspector or above. The requests for the more intrusive types of communications data must be approved at Superintendent level or above. The inspections have established that generally a good level of independence and objectivity exists in the approvals process and generally designated persons in police forces and law enforcement agencies are discharging their statutory responsibilities effectively. Each application must be vetted by an accredited officer before it is submitted to the Designated Person for approval.

3.33 During the reporting year the National Policing Improvement Agency (NPIA) took over responsibility for the training and accreditation of SPoC staff. I still believe it is very important that all staff who are involved in the acquisition of communications data are well trained and that they maintain their skills levels to the best possible standards. My Inspectorate has a very close working relationship with ACPO DCG and senior policymakers in the Home Office who formulate policy and co-ordinate all matters relating to communications data with public authorities, industry and other external agencies such as the NPIA. A new SPoC accreditation course has been developed by the NPIA and this focuses much more upon the practical elements of acquiring communications data and the role and responsibilities of the accredited staff who play a key role in ensuing every public authority acts in an informed and lawful manner. My Chief Inspector and one of the Inspectors met the NPIA during the development stages and the good practice which we have uncovered during the inspections has been taken into account.

3.34 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 failure to exercise 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. Relevant staff in police forces and

law enforcement agencies have responded positively to the inspections and they understand that they are an essential part of my oversight responsibilities. Police forces and law enforcement agencies are now well accustomed to dealing with the legislation and the results from this year's inspections are very heartening. There is clear evidence from the inspections that the SROs and the vast majority of their staff are committed to providing the best possible level of service and achieving good adherence to the Act and Code of Practice.

*Intelligence Agencies*

3.35 The intelligence agencies are subject to the same type of inspection methodology and scrutiny as police forces and law enforcement agencies. For the most part the work of the intelligence agencies is highly sensitive and secret, and this limits what I can say about their inspections.

3.36 During the reporting year the Security Service, Secret Intelligence Service and Government Communications Headquarters were all inspected by my Chief Inspector and one of the Inspectors. They all emerged very well from the inspections and the inspection team concluded that they are achieving a good level of compliance with the Act and Code of Practice. Of all the intelligence agencies the Security Service is the largest user of communications data and it has a fully automated system to manage its requirements.

3.37 Communications data is used extensively by the intelligence agencies, primarily to build up the intelligence picture about persons or groups of persons, who pose a real threat to our national security. Given the nature of their work it is unavoidable that there will be some degree of collateral intrusion into the private lives of persons who have had contact with the subjects of their investigations. However, this is recognised by the intelligence agencies from the outset and the inspections have shown that it is being managed to the best of their ability. The error rate of all the intelligence agencies is very low in comparison with the number of requests which are processed for communications data.

*Local Authorities*

3.38 There are approximately 433 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. However, local authorities may acquire communications data for the purpose of preventing and detecting crime, although 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.

3.39 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.

3.40 Local authorities are required to adhere to the Code of Practice and requests for communications data are approved at a senior level, the level having been enhanced by recent changes to the legislation. In most cases this has been the head of the trading standards service or the head of the environmental health department or housing benefits sections although solicitors have also often been 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

the infrequent use which most Councils make of their powers sometimes makes it difficult for relevant members of staff to keep abreast of developments in the communications data community. I am pleased that the Home Office has provided funding to the National Anti-Fraud Network (NAFN) and it is able to provide a national SPoC facility to all of its members. During the reporting year we have encouraged local authorities to make use of the facility, as the accredited staff at NAFN have been trained to the same standards as their counterparts in the police. One of my Inspectors has already visited NAFN and the systems and processes are being maintained to a good standard. Local authorities can use the facility with confidence and in the full knowledge that the data will be obtained in accordance with the law. Of course the Designated Person in the local authority still has responsibility for approving the application for communications data but the accredited staff in NAFN scrutinise it independently and this should weed out any which are unnecessary or unjustified.

3.41 During the period covered by this report 131 local authorities notified me that they had made use of their powers to acquire communications data, and this is slightly more than last year. A total of 1,756 requests were made for communications data and the vast majority were for basic subscriber information, although 24 Councils reported that they had acquired some service use data under Section 21(4)(b) of the Act. The total number of requests for communications data is marginally above last year's figure. Virtually all of the local authorities, which have used their powers, have been inspected at least once since the legislation was introduced. The core activities of the trading standards service and environmental health teams are now centralised in a number of the larger local authorities and therefore it is easier for them to manage the process of acquiring communications data. My Inspectorate identified the largest users of communications data at an early stage and they are inspected more regularly.

3.42 During the reporting year 31 inspections of local authorities were conducted. Six of these were inspected for the first time, either because they had notified me that they had started to make use of their powers, or because they were acquiring communications data on a more frequent basis. Twenty one of the local authorities were inspected for a second time and the remaining four were inspected for the third time. Seventeen of the local authorities which were inspected had made use of service use data and generally the Inspectors were satisfied that it was necessary to obtain it and it was proportionate to the investigative objectives. However, one of the local authorities was criticised for obtaining this type of data before carrying out checks to identify the relevant subscribers. At that stage in the process there was no information or intelligence to indicate whether the telephone numbers or their subscribers were associated with criminal or illicit activity and potentially they could have been innocent members of the public who were in contact with the suspect for perfectly legitimate reasons. Changes have been made to the working practices of the local authority concerned, and they will ensure that service use data is acquired correctly in future. I will give some examples of how the local authorities use communications data later in this section of the report.

3.43 I am aware that some sections of the media continue to be very critical of local authorities, and there are allegations that they often use the powers which are conferred upon them under RIPA inappropriately. However, I can state that no evidence has emerged from the inspections, which indicates communications data is being used to investigate offences of a trivial nature, such as dog fouling or littering. On the contrary it is evident that good use is being made of communications data to investigate the types of offences which cause harm to the public and to which I have already alluded in paragraph 3.40 above.

3.44 Twenty three of the local authorities had achieved good or better standards and the remaining eight were satisfactory. It was good to see that the recommendations from the previous inspections had always been fully implemented and where necessary improvements had been made to the systems and processes. My Inspectors found two instances of local authorities obtaining incoming call records,

and these constitute errors because Councils are not lawfully entitled to acquire this type of data. The Inspectors were satisfied that these errors were caused as a result of a genuine misunderstanding and not through any wilful or reckless attempt to circumvent the legislation. Most of the staff in the CSPs are aware that they must not comply with requests from local authorities for traffic data, but inevitably one or two may slip through the net. In both the above cases the errors were drawn to the attention of the SROs in the local authorities concerned and action has been take to prevent any similar errors occurring in the future. Incidentally, the number of errors reported by local authorities last year was ten and this equates to about 0.01% of the requests made. I have not encountered any cases which would be serious enough for me to invoke the powers which I have outlined previously in paragraph 3.35 of this report.

3.45 In three of the inspections technical breaches of the Act and Code of Practice were found and this meant that a small amount of data was not obtained fully in accordance with the law. Nevertheless my Inspectors were satisfied that they had no bearing on the justifications for acquiring the data and the data had been used for a correct statutory purpose. My Inspectors looked at the use which local authorities had made of the communications data, as this is a good check that they are using their powers responsibly. They concluded that effective use was being made of the data to prevent and detect crime. Wolverhampton City Council acquired communications data to investigate the large scale manufacture and distribution of counterfeit media products via the Internet and computer fairs. The offender was convicted and sentenced to three years imprisonment. The estimated loss to legitimate businesses was in the region of £1 million and this was stopped when the four counterfeiting factories were dismantled. The Central England Trading Standards Regional Scambuster Team based at Solihull Borough Council, and West Midlands Police jointly investigated a rogue builder when complaints were received from two members of the public that they had been ripped off. Initially the Crown Prosecution Service advised against going to trial because there were only two victims and it would therefore be difficult to prove the full extent of his criminality. Outgoing call records were obtained in relation to the suspect's phone and this enabled the investigation team to identify a number of other victims who were prepared to give evidence, many of whom had been unaware that they had actually been the victim to a fraud. The offender obtained approximately £200,000 by fraud from his victims over an 18 month period. The case was eventually tried in Birmingham Crown Court and the offender pleaded guilty and was sentenced to 4 years imprisonment. It is extremely unlikely that he would have been brought to justice if the investigating officers had not made effective use of the powers to acquire communications data.

3.46 Communications data is a powerful investigative tool but it must always be used responsibly and all persons within the process must ensure that they act fully in accordance with the law. The local authorities appreciate that I oversee the use of their powers and the inspections ensure that they comply with the Act and Code of Practice.

*Other public authorities*

3.47 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 (MHRA), to name just a few.

3.48 During the course of the reporting year inspections were carried out at the Environment Agency, Gambling Commission, Defra Investigation Services, Financial Services Authority, Police Ombudsman of Northern Ireland, Royal Mail, Maritime and Coastguard Agency, Criminal Cases Review Commission, National Offender Management Service, Serious Fraud Office, Ofcom and the Independent Police Complaints Commission. Half of these public authorities were inspected

for the third time and the others have had two inspections since the legislation was introduced.

3.49 By comparison with police forces and law enforcement agencies the above mentioned public authorities make very limited use of their powers to acquire communications data. For example, the public authorities, which are named in the preceding paragraph, made a total of 2,259 requests for communications data. The largest user by far was the Financial Services Authority with 1,705 requests for data. Eleven errors were reported by the above mentioned public authorities during the same period. One of these errors was found during the inspection of Defra as a log on history had been obtained for an Internet Protocol Address. This constitutes traffic data and Defra is not allowed to acquire this type of data under the Act. Defra only made three applications for communications data during the course of the year and the accredited staff had genuinely not realised that they had made a request which was unlawful. Action has been taken to prevent this type of error occurring in the future.

3.50 With the exception of the National Offender Management Service (NOMS) all of the public authorities emerged well from the inspections and the Inspectors were generally satisfied that communications data was being acquired lawfully and for a correct statutory purpose. I should clarify that the National Offender Management Service was not acting unlawfully but its systems and processes needed to be maintained to a much better standard and a series of recommendations were made to help them do so. The Director of NOMS has since informed us that the recommendations have been implemented.

3.51 Generally the inspections confirmed that the above mentioned public authorities acquire communications data for specialist purposes and they use their powers responsibly. For example, the Royal Mail had made good use of communications data to investigate Parcel Force employees who were stealing items from the postal system. The Environment Agency had used communications data to investigate unlicensed landfill sites and related offences under Section 33 of the Environmental Protection Act. The MHRA mainly acquired subscriber information to identify persons who were involved in the supply and distribution of unlicensed, unlawful or counterfeit medicines and medical devices which could cause harm or loss of life.

# Section 4: Interception in Prisons

## General

4.1 At the request of the Secretary of State I have continued to provide 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. Last year my non-statutory oversight responsibilities were extended to cover the three prisons which operate in Northern Ireland. Only one of the prisons in Northern Ireland was inspected and it was sustaining a good level of compliance.

4.2 The interception of prisoners' telephone calls and correspondence is permitted, and in some 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 YOIR 11(4). Interception is mandatory, usually in the case of High Risk Category A prisoners and prisoners who have been placed on the Escape List. Often it is necessary to monitor the communications of prisoners who have been convicted of sexual or harassment offences, and who continue to pose a significant risk to children or the public. 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.

4.3 All prisoners are allocated a PIN number in order that they may use the Pin-phone facility to maintain contact with friends or family whilst they are in custody. They must be informed verbally and in writing that their communications are subject to interception and they must complete a contacts list which separately identifies any numbers which should be placed on the confidential side of their Pin-phone account. The telephone numbers of legal advisers will then be entered into the Pin-phone system in such a way that any calls to these numbers will automatically not be recorded. Generally this should act as a good safeguard and prevent any legally privileged conversations being monitored unintentionally but it is not totally failsafe. Towards the end of last year the Prison Service introduced new measures which are designed to prevent breaches of Articles 6 and 8 of the Human Rights Act. In reality the system still relies heavily upon manual intervention, and so no guarantee can be given that a breach will never occur in the future. However, providing the prisoners and their lawyers always adhere to the rules and the prison staff apply the process diligently the risk of legally privileged communications being intercepted will be minimised.

4.4 As part of the new measures the Chief Operating Officer issued a new version of the Communications Compact, together with a directive that a copy must be provided to each prisoner who enters a prison establishment. It also contains a section where the prisoner must provide the contact numbers of his legal advisers so that they can be checked and then placed on the confidential side of the Pin-phone account. Serious weaknesses and failings were found in this aspect of the process during the inspection of 52 prison establishments this year and this must be a cause for concern. In two instances the Communications Compact was not in evidence at all and fourteen establishments had failed to introduce the current version. Seven establishments were not carrying out checks on the legal contact numbers and the remaining 29 establishments were failing to follow the correct procedures for issuing and filing the document. Following these inspections a recommendation was made to remedy the failings and weaknesses and the Governors in each of these establishments have since assured me that they have been implemented. Nonetheless about 50 prison establishments have still to be inspected since the new measures were introduced and I cannot predict with any degree of confidence that they will be fully compliant with this important aspect of the process.

## Work of the Inspectorate during the period covered by this report

4.5 There are 139 prisons in England & Wales and since the Inspectorate was formed virtually all of them have been inspected at least twice. Prisons in the High Security Estate are generally subject to an annual inspection but the frequency of inspections of other establishments depends on their previous level of compliance.

4.6 During the period covered by this report my Inspectors visited 88 prisons which roughly equates to two thirds of the whole estate. This number includes 4 prisons which were visited twice during the year because very serious failings were found in the systems and processes for conducting the interception of communications. 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.

4.7 Lawful monitoring carried out in accordance with published criteria can help to safeguard the public, the prison, its staff and other prisoners. It requires good practice by well trained, well led and dedicated staff. This must be supported by a sound infrastructure incorporating good quality documentation capable of being completed to the highest standard in order to provide clear and unambiguous audit trails.

4.8 Forty one of the prisons emerged well from the inspections and the overall level of compliance with the rules was good or very good. Indeed the Inspectors found examples of good practice which are now firmly embedded in the systems and processes and managers and staff clearly demonstrated a commitment to achieve the best possible standards. The prisons which have a dedicated team of well trained staff to conduct the interception of communications always achieve much better standards and we always advocate this as best practice.

4.9 Regrettably very serious weaknesses and failings were found in the systems and processes of 24 of the prison establishments which were inspected. The other 19 establishments fared a little better but nevertheless failings and weaknesses were also found during their inspections. This number is too high and it indicates a failure by managers and staff to ensure that the interception of communications is conducted fully in accordance with the rules. Failure to do so could potentially place children, vulnerable prisoners, members of the public and prison staff in harm's way and managers have been warned that they could then find themselves in an indefensible position. Having said that I do not imply that prison managers and their staff are deliberately setting out to circumvent the rules. Often these failings result from a lack of equipment and resources to conduct the interception efficiently and effectively, especially when large numbers of prisoners need to be monitored because they are considered a risk to children or are subject to harassment restrictions. However, these failings often occur because the monitoring staff lack clear leadership, direction and supervision and this can easily be remedied.

4.10 In quite a number of establishments the monitoring of prisoners who pose a risk to children or the public is still a weak area. For example, in one establishment in the High Security Estate the Offender Management Unit (OMU) had decided that the telephone calls and correspondence of 476 prisoners needed to be monitored. This target was completely unrealistic and unattainable and a huge increase in staff and equipment would be necessary to ensure the monitoring was conducted efficiently and effectively. The Prison Service simply does not have the funding to pay for this, and I am not convinced that it would be money well spent. The setting of targets must be geared to the level of risk which the prisoners pose, and the equipment and resources that are available, otherwise the monitoring staff will not be able to prioritise their work. In my judgement each establishment must try to adopt the most tenable position it can, given that there may be a large number of individuals who pose a risk to children or are subject to harassment restrictions. In some instances this may not always be the best position, but good evidence should be created to show that the risk factors have been taken into account, as far as possible, and that is all that can be achieved in the prevailing circumstances.

4.11 Fortunately my Inspectors have not found any evidence of harm to children or members of the public who need to be protected from these prisoners, but the whole process could be managed much better. At the beginning of the year a new version of the National Security Framework (NSF) was issued and it now stipulates that Interception Risk Assessments must be introduced into the process. Various factors now have to be taken into account in the Interception Risk Assessment before an authorisation is granted to monitor a prisoner's communications. The introduction of the Interception Risk Assessments creates good evidence to support the Authorising Officer's decision whether monitoring is necessary or not. If an authorisation is produced to conduct offence related monitoring then the Authorising Officer must have a clear expectation that the communications will be properly evaluated. I am pleased to say the introduction of the Interception Risk Assessments is already having a marked effect and they are enabling the Offender Management Units to reduce the number of prisoners who actually need to be monitored. The monitoring staff are then able to focus their efforts upon the prisoners who pose the highest risk. Individuals can be moved back onto the monitoring list at any time if fresh intelligence indicates that they pose an increased risk to children or the public, or immediately before their release, or transfer to another establishment, to establish their mindset. The information gathered from

the interception can then be made available to the police and probation service so that they can take any action which may be necessary when the prisoner re-enters the community.

4.12 The inspections have also revealed that an alarming number of Category B local prisons appear to have a very limited capacity to monitor prisoners who pose a real threat to good order and security and this is a cause for concern. The smuggling of drugs and illicit mobile telephones are serious problems for most prisons, irrespective of their security status, and if a serious incident were to occur, which could have been prevented through the gathering of intercept intelligence, then prison managers and staff could find themselves in an indefensible position. Regrettably on occasions my Inspectors still have to emphasise this point in a number their reports.

4.13 The Category B local prisons, which were inspected during the reporting period, were asked to provide details of the numbers of illicit mobile telephones and associated equipment that had been seized in a six month period. Statistics from 25 prisons were collated and these revealed that 1,456 mobile telephones and 797 SIM cards were seized. Under the Offender Management Act 2007 and Prison Order 1100 dated 26 March, 2008 it is now a criminal offence to convey a mobile telephone or a component part of this equipment into a prison without the authorisation of the Governor and 11 of the prisons were making use of this legislation. However, the availability of such a large number of illicit telephones in the prison system is a serious cause for concern because prisoners can also use them to access the Internet.

4.14 Following the publication of the Blakey report in 2008 the Chief Operating Officer issued the Mobile Phones Good Practice Guide which was designed to help prisons minimise the number of mobile phones entering prisons and disrupt the number of mobile telephones that they were unable to find. Intelligence from the Pin-phones does help to prevent and detect attempts to smuggle them into the prison and this was part of the strategy. Clearly quite a number of the establishments are unable to implement the strategy fully because the resources and equipment are weighted far too heavily in favour of the offence related monitoring and this is a continuing problem. It is crucially important that prisoners are prevented from using mobile telephones to conduct criminal or illicit activity inside and outside the prison. Better use of the Interception Risk Assessments will eventually reduce the amount of offence related monitoring which needs to be conducted and this will in turn increase the capability to conduct more intelligence-led monitoring.

4.15 The Inspectorate has an excellent working relationship with the Prison Service National Intelligence Unit (NIU) and regular meetings are held to review the outcomes of the inspections. All the inspection reports are copied to the NIU and the Directors of Offender Management in the regions. My Chief Inspector also attends high level meetings of the Audit and Inspection Group chaired by NOMS Audit and Corporate Assurance, where representatives from the National Audit Office, Her Majesty's Inspectorate of Prisons and others meet to discuss issues of common interest. In previous inspection reports I mentioned that the Prison Service intended to trial a new pilot scheme which will test the effectiveness of the systems and processes for conducting the interception of communications. I understand this is scheduled to commence in May 2010 and hopefully the results will be available for the Secretary of State and Director General to consider later in the year.

# 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 2.32 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 the light of technical and administrative developments. I did not see nor was I asked to comment on any revised handling arrangements during the period of this Report.

# 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, four senior members of the legal profession served on the Tribunal for the whole of 2009, with four additional new members being appointed in July 2009.

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 157 new applications during the calendar year 2009 and completed its investigation of 58 of these during the year as well as concluding its investigation of 67 of the 75 cases carried over from 2008. 107 cases have been carried forward to 2010.

## 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. My assistance was not sought by the Tribunal during 2009.

## Determination made by the Tribunal in favour of a complainant

6.4 During 2009 the Investigatory Powers Tribunal made one determination in favour of a complainant. This is the fourth occasion since its inception that the Investigatory Powers Tribunal has upheld a complaint. On the grounds of confidentiality, the Investigatory Powers Tribunal Rules 2000 prohibit me from disclosing specific details about the complaint, but it is sufficient to say that the conduct complained of was not authorised in accordance with the relevant provisions of RIPA.

# Section 7: Conclusion

7.1 As I said in my previous Reports, 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 would also like to say 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.


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

**The Parliamentary Bookshop**
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

**TSO@Blackwell and other Accredited Agents**

**Customers can also order publications from:**
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Tel 028 9023 8451  Fax 028 9023 5401

ISBN 978-0-10-296842-2