# 2010 Annual Report of the Interception of Communications Commissioner

## 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
30 June 2011

Laid before the Scottish Parliament by
the Scottish Ministers
June 2011

HC 1239
SG/2011/117

£15.50

# 2010 Annual Report of the Interception of Communications Commissioner

## 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
30 June 2011

Laid before the Scottish Parliament by
the Scottish Ministers
June 2011

HC 1239
SG/2011/117

£15.50

London: The Stationery Office

Any enquiries regarding this publication should be sent to us at the office of the Interception of Communications Commissioner

2 Marsham Street, London, SW1P 4DF

This publication is available for download at www.official-documents.gov.uk.

ISBN: 9780102974072

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

ID P002439221 06/11

Printed on paper containing 75% recycled fibre content minimum.

**The Right Honourable Sir Paul Kennedy**

Interception of Communications Commissioner
2 Marsham Street
London
SW1P 4DF

8th June 2011

The Rt. Hon David Cameron
10 Downing Street
London
SW1A 2AA

I enclose my fifth Annual Report, covering the discharge of my functions as Interception of Communications Commissioner between 1st January 2010 and 31st December 2010. I have followed past practice and submit the report in two parts; in addition to the main report there is a Confidential Annex containing information the disclosure of which I believe would be prejudicial to national security, the detection or prevention of serious crime or to the economic well-being of the UK. Once again I leave it to you, as Prime Minister, to decide whether to accept this approach and how much of the report to make available to the public.

In the interests of transparency I have taken on board useful feedback on my previous annual reports from a variety of interested parties. Therefore this year's report focuses more on the nature of my inspection visits, the process underpinning the authorisation of interception, details of errors reported by agencies and, crucially during a period of potential reform of intelligence oversight, improvements in working practices that occur through the constructively challenging relationship I enjoy with those agencies and public authorities whose activities I oversee.

I hope that this meets with your approval.

**Sir Paul Kennedy**

# CONTENTS

# 1. THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER

**Sir Paul Kennedy**

Sir Paul Kennedy had a long and varied legal career prior to being appointed the Interception of Communications Commissioner on 11th April 2006. Born in 1935, Sir Paul was called to the Bar by Gray's Inn in 1960 and took silk in 1973. He served as a Justice of the High Court, assigned to the Queen's Bench Division, from 1983 to 1992. Sir Paul was the Presiding Judge of the North Eastern Circuit from 1985 to 1989. He then served as a Lord Justice of Appeal from 1992 to 2005 and as Vice-President of the Queen's Bench Division from 1997 to 2002. Sir Paul has been a member of the Court of Appeal in Gibraltar since 2006, and is a member of the Advisory Board of Youth at Risk.

## The role of the Commissioner

1.1 I was appointed to the role of Interception of Communications Commissioner on 11th April 2006. My appointment was made by the Prime Minister initially for a period of three years under Section 57 of the Regulation of Investigatory Powers Act (RIPA) 2000 The initial period was extended on 11th April 2009 for a further period of 3 years until 10th April 2012.

1.2 In Summer 2010 Sir Peter Gibson, then Intelligence Services Commissioner, and I asked the Home Office to consider aligning appointments of the Commissioners to match the statutory Annual Report periods. Later in 2010 we were both pleased to hear that the Home Office was content to make this change. Therefore, when my current term expires, and providing the Prime Minister is content to reappoint me for a further term, I will remain in post for a period of just over 8 months from 11th April 2012 to 31st December 2012. My successor will therefore be appointed from 1st January 2013 and I look forward to serving this additional term.

## An introduction to RIPA

1.3 As I have said, I was appointed under section 57 of RIPA. The coming into force of the Act on 2nd October 2000 coincided with that of the Human Rights Act 1998 (HRA), which incorporated the European Convention on Human Rights (commonly known as the ECHR) into UK law.

1.4 RIPA is a broad and not always well-understood piece of legislation. The introduction of both RIPA and the HRA brought about a number of changes in the law and the practice of those responsible for lawful interception in the UK. The legislation has also put into statutory form the roles of the Interception of Communications Commissioner, the Intelligence Services Commissioner, the Surveillance Commissioner and the Investigatory Powers Tribunal. The 2000 Act updated the Interception of Communications Act 1985 in light of the Human Rights Act 1998 and also required oversight of a number of investigatory techniques.

1.5 It is important to appreciate that the 2000 Act regulates interception, which is a valuable tool, not only in relation to the prevention and detection of acts of terrorism and other national security interests but also, as the Act makes clear, for the prevention and detection of serious crime and in order to safeguard the economic well-being of the UK. The powers must only be invoked when it is necessary and proportionate to do so, and safeguards are embodied in the Act to achieve that end.

**Figure 1: RIPA summary box interception**

| **Regulation of Investigatory Powers Act (2000)** | | | | | |
|---|---|---|---|---|---|
| • Enacted on 2nd October 2000<br>• Updated the Interception of Communications Act (1985), Intelligence Services Act (1994) in light of the Human Rights Act (1998)<br>• Put into statute roles of Interception of Communications Commissioner, Surveillance Commissioner, Intelligence Services Commissioner and the Investigatory Powers Tribunal | | | | | |
| **Which section of RIPA?** | **What is the Power?** | **What is a typical use of this Power?** | **When can this power be used?** | **Who can use the power? *** | **Who authorises and who oversees the responsible use of power?** |
| Pt. I Chapter I | Interception of an individual's communications (i.e. telephones, emails, texts, post ) | A law enforcement agency (LEA) intercepting an individual's phone calls | In the interests of national security<br>Prevention and detection of serious crime<br>Safeguarding the economic well-being of the UK | Intelligence agencies<br>Serious and Organized Crime Agency (SOCA)<br>Metropolitan Police (Met)<br>Police Service for Northern Ireland (PSNI)<br>Scottish Police<br>Scottish Crime and Drug Enforcement Agency (SCDEA)<br>HM Revenue and Customs (HMRC)<br>Defence Intelligence Staff (DIS) | Warrant signed by the Home Secretary, Foreign Secretary, Northern Ireland Secretary or Scottish Ministers<br>Oversight provided by Interception of Communications Commissioner |

| | | | | | |
|---|---|---|---|---|---|
| Pt. I Chapter 2 | The acquisition of communications data ( the who, where, what and when of a communication) | Police forces and law enforcement agencies obtaining itemised phone records to show contact between suspects, prove association and/or a conspiracy in relation to serious crimes (i.e. murder, supply and distribution of Class A drugs). Local authorities acquiring subscriber data to ascertain the ownership of a mobile phone used by a rogue trader, illegal money lender or fly-tipper | Mainly used in relation to the prevention and detection of crime or the prevention of disorder or in the interests of national security. For a full list of the statutory purposes under which the powers can be used refer to Section 22(2) of RIPA. | Mainly used by police forces, intelligence agencies, other law enforcement agencies such as Her Majesty's Revenue & Customs and the Serious and Organised Crime Agency, and other public authorities such as the Royal Mail, Environment Agency and local authorities. For a full list of the public authorities that can acquire communications data refer to Statutory Instrument 2010 No. 480 which is made available at the following link http://www.legislation.gov.uk/uksi/2010/480/pdfs/uksi_20100480_en.pdf | A senior member of that authority<br><br>Oversight conducted by the Interception Commissioner through a team of Inspectors reporting annually. (See section 7 of the current report). |

| | | | | | |
|---|---|---|---|---|---|
| Chapter 3 | The investigation of electronic data protected by encryption | Request for encryption password or key pertaining to criminal suspect's computer | Interests of national security<br>Prevention/ detection of crime<br>Interests of economic well-being of United Kingdom; or<br>For the purpose of securing the effective exercise or proper performance by any public authority of any identified statutory power or statutory duty | Any public authority | Authorisation is most frequently by a Judge, except when authorised by a judicial authority, oversight is conducted by the Interception of Communications, Intelligence Services and Surveillance Commissioners. |

* The main public authorities with interception and communications data powers are listed here, further details and links to relevant statutory instruments are available in Annex A to this report

**My areas of oversight**

1.6 My role is tightly defined in RIPA; Section 57 (2) of the Act provides that I keep under review the following:

- The exercise and performance by the Secretary of State of the power and duties conferred upon him (or her) under sections 1 to 11
- The exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties under chapter II of part 1 of the Act in relation to the acquisition of communications data. This year's assessment of my function in relation to communications data is detailed in the second half of this report. Put simply, this is my assessment, through a team of Inspectors, of the performance of those bodies (such as security services, police forces, local authorities and others) which can request information as to the 'who, where and when' of a communication, be it a letter, a phone call or a text message. We check that those bodies are using their powers legally and responsibly.
- 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
- The adequacy of the arrangements by virtue of which:
  - The duty which is imposed on the Secretary of State by section 15; and
  - So far as applicable to information obtained under Part I, the duties imposed by section 55 are sought to be discharged,

In essence my Inspectors and I act as auditors. We look at the materials on which decisions were made, how that material was processed, and consider whether the decision was necessary and proportionate. Also in many cases we are able to see what was achieved as a result.

1.7 It is also my function under RIPA to give the Investigatory Powers Tribunal, also set up under RIPA (s.65), such assistance as may be necessary in order to enable it to carry out its functions. The Tribunal hears complaints in relation to the use of RIPA powers. In practice my assistance has rarely been sought, and it was not sought at all in 2010, but when sought it has willingly been given.

1.8 Part III of RIPA details my oversight function in respect of encryption. Encryption is defined as the scrambling of information into a secret code of letters, numbers and signals prior to transmission from one place to another. Encryption is used not only by criminals and terrorists but also by hostile foreign intelligence services to further their interests.

## Non-statutory oversight

1.9 My predecessor was asked by the Secretary of State to undertake oversight of some types of interception not covered under the 2000 Act, such as the interception of the mail and telephone calls of serving prisoners, which is subject to other legislation. He agreed to undertake that oversight and I have acted in accordance with that agreement.

## This year's annual report

1.10 Readers interested in my area of intelligence oversight will be aware that the structure of the 2010 report is somewhat different to previous years. I have attempted, based on useful feedback over the years from readers and the media, to include in this year's report more details of:

- Where security restrictions allow, practical examples and case studies related to areas of my oversight, in particular with regard to the acquisition of communications data and the process of signing authorisations and warrants
- Year on year changes in errors and statistics from the security, intelligence and law enforcement agencies.
- In relation to errors that have occurred, where possible a greater focus on what has been learnt and the system changes which have occurred to reduce the risk of a recurrence.
- A greater assessment of the impact of technology on interception and views on the future of intelligence oversight overall.
- More detailed findings / conclusions from the inspections conducted.

1.11 This is my fifth annual report and it covers the period between 1st January 2010 and 31st December 2010. I follow the practice of my predecessor in preparing an open version of my annual report, which I expect to be published, and which includes the broad changes in emphasis highlighted above. For obvious reasons some matters cannot be published, and they appear in the Confidential Annex to this report.

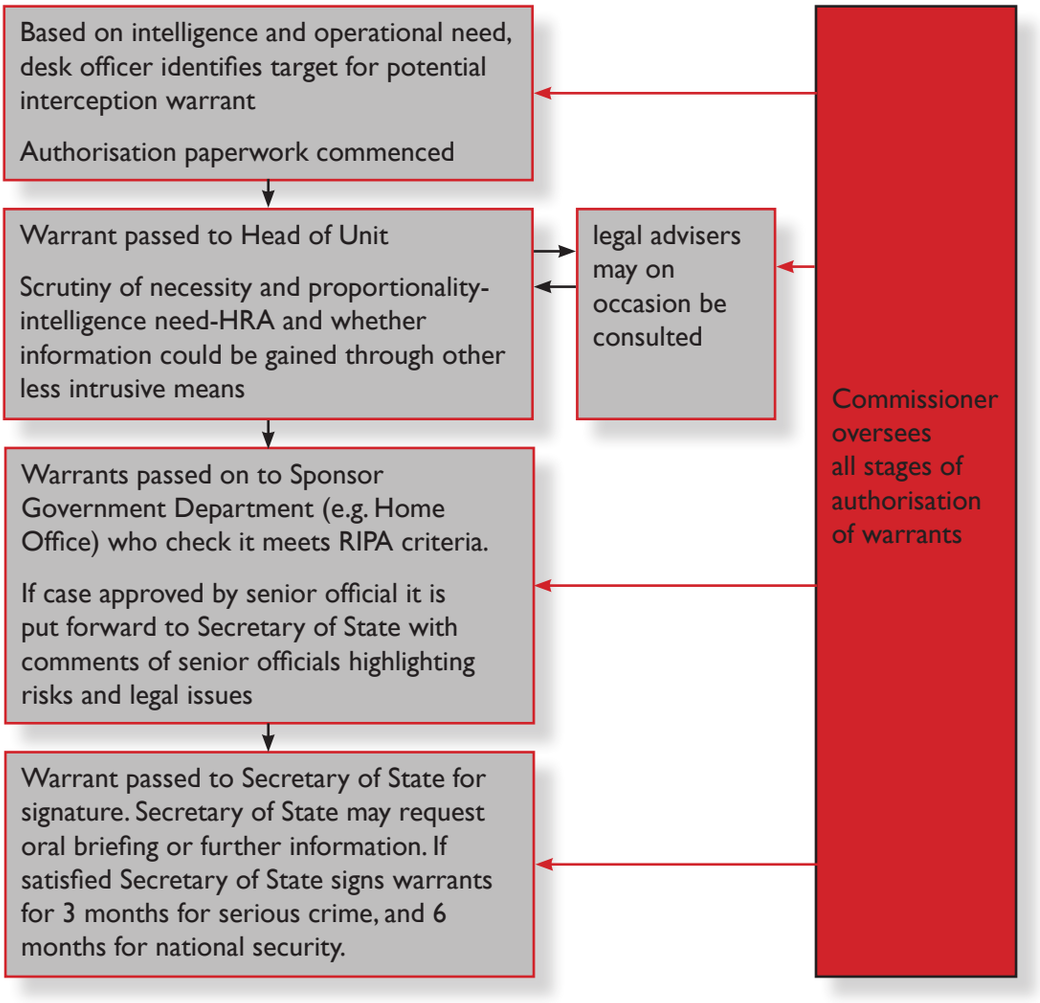
# 2. PART 1 CHAPTER 1: THE INTERCEPTION OF COMMUNICATIONS

**What is interception?**

2.1 Interception of communications is amongst a range of investigative techniques used by security and law enforcement agencies for the prevention and detection of acts of terrorism, in the interests of national security, for the detection of serious crime and to safeguard the economic well-being of the UK (where this is directly related to national security)

2.2 Due to the potential level of intrusion into an individual's private life associated with interception, RIPA requires that interception of communications can only be authorised by a warrant signed by a Secretary of State or the Scottish Ministers[1]. The authorisation can only be given in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom

**Figure 2: The warrantry authorisation process**




1 Scottish Ministers are the appropriate authority in terms of serious crime in Scotland

## The role of the Secretary of State

2.3 As detailed in the relevant diagram, the role of the Secretaries of State and Scottish Ministers as democratically elected individuals signing off acts which may involve intrusion into the private life of citizens is, in my view, crucial. So my predecessors and I have held annual meetings with Secretaries of State in the Home Office, Foreign and Commonwealth Office, Northern Ireland Office, Ministry of Defence and with the Cabinet Secretary for Justice in Scotland. I continued with this practice in 2010, and met all but one of the relevant Secretaries of State in the new Westminster administration in November and December.

2.4 It is clear to me that Secretaries of State and the Scottish Ministers spend a substantial amount of time and effort considering operational merits, necessity, proportionality and wider implications before signing off warrants that authorise interception. Although Secretaries of State and the Scottish Ministers are provided with in-depth submissions before signing authorisations, if they wish to have further information in order to be satisfied that they should grant the warrant then it is requested and given. The outright refusal of an application is rare, mainly because an authorisation request crosses the desks of a number of officials and, in certain circumstances, legal advisers and is scrutinised with some considerable care before it reaches the Secretary of State or the Scottish Minister. A final comment recommending signature or highlighting risks is made by someone at Senior Official or Director Level in, for example, the Home Office or Foreign Office prior to submission to the relevant Secretary of State or Scottish Minister. Overall I am confident that, as the agencies are aware, the Secretary of State and the Scottish Ministers are not simply 'rubber-stamping' requests presented to them.

## How are my Inspections conducted?

2.5 This year I have continued the practice of undertaking twice-yearly inspection visits to each of the following organisations during the summer and early winter.

- Security Service
- The Secret Intelligence Service (SIS)
- GCHQ
- SOCA
- Metropolitan Police Counter Terrorism Command
- Police Service Northern Ireland
- Northern Ireland Office
- Her Majesty's Revenue and Customs (HMRC)
- Foreign and Commonwealth Office (FCO)
- Home Office
- Scottish Government
- Ministry of Defence

2.6 The way in which my inspection visits are conducted is illustrated in the next diagram. During these visits I take the opportunity to meet officers within the agencies and departments who are involved in the formation and authorisation of intercept warrants. I also meet those who receive and disseminate intercepted product. I am also often briefed on the overall security threat situation and other broader policy issues, which provides the context for the warrants I review

2.7 My role is essentially that of a retrospective auditor of warrants, lists of which are presented to me some weeks prior to the visit itself. The agencies and departments provide a full list of all warrants extant, modified or cancelled since the previous visit. I then make my selection. I am satisfied that the agencies provide me with a full list of authorisations, and they often highlight particularly challenging warrants, and those that have been associated with compliance errors ,to help me to decide which warrants to review.

**Figure 3: An inspection visit**

| **Each Government Department or Agency authorising warrants for interception is visited twice annually** | |
|---|---|
| **Stage** | **Purpose** |
| **Selection Stage** | |
| Warrant-Issuing Department (WID) or LEA provide list of extant, expired and modifications to authorisations since last inspection visit. | Checks are made by WID and Secretariat to ensure all authorisations are submitted |
| Agencies also commonly refer Commissioner to specific cases of interest concerning either errors or legal issues | Commissioner may raise specific cases for subsequent reading day prior to inspection day itself |
| Commissioner dip-samples a number of warrants and authorisations for further scrutiny on inspection day | To ensure the random nature of inspections and ensure all warrants have an equal chance of being selected for review |
| **Inspection Day (approximately 1 month later)** | |
| Day spent in the WID/Agency being briefed by Senior Officials on threat/ emerging policy issues | To provide Commissioner with a general operational overview as to the nature of the threat in relation to which applications for authorisations |
| Reading through and scrutinising warrantry paperwork | Commissioner seeks to reassure himself that throughout authorisation process principles of necessity, proportionality and other RIPA safeguards are being applied |
| Where necessary, oral briefings by case officers to detail intelligence case behind the submissions and answer Commissioner's questions on any errors | Specific focus on ensuring renewals are being submitted in good time and that urgent oral applications really are urgent |
| **Follow-up stage** | |
| Meetings with Secretaries of State or Scottish Ministers | Ensure getting best value from Commissioner's expertise |
| Report of inspections within Annual Report | Characteristic of an effective relationship between Commissioner and agencies |
| Potential informal consultation between Agency and Commissioner on challenging legal or policy issues | |

2.8 In the course of my visit I seek to satisfy myself that those warrants selected fully meet the criteria set out in RIPA, that proper procedures have been followed and that the relevant safeguards within the Codes of Practice have been adhered to. During the visits I not only review the actual warrants and supporting paperwork, but, as and when necessary, discuss the rationale behind the warrants with the officer concerned. I am also able to view the product of any interception that may have been authorised. It is of the utmost importance to ensure that the facts justified the use of interception, and that principles of necessity and proportionality are adhered to.

2.9 Throughout my 2010 visits, as in previous years, I continued to be impressed by the quality, fairness, dedication and commitment of the personnel carrying out this work. Irrespective of the level of threat, officers continue to show an intimate knowledge of the legislation surrounding interception, how it applies to their specific areas of work, and they are keen to ensure they comply with the legislation and appropriate safeguards. The risk of defective applications in my opinion remains very low due to the high level of scrutiny that I believe is applied to each authorisation as it crosses a number of desks in the warrantry units of the Home Office, Foreign Office Ministry of Defence, Northern Ireland Office and Scottish Office, before reaching the relevant Secretary of State.

2.10 It is my belief that my relationship with the agencies and departments I oversee is based on equal levels of trust, mutual understanding and constructive comment. Throughout the course of my inspections I have never had to demand access to files and indeed have been provided with more operational detail behind warrants than is strictly necessary. This enables me to form a better assessment of the necessity and proportionality behind applications for interception. I believe the agencies welcome my oversight and on occasions they consult me before particularly complex operations and investigations. It is my belief that the public should have confidence in the integrity of both the agencies and my oversight role.

2.11 I will refer in the sections that follow in some detail to the specific kinds of errors reported to me during the period under review. However, when errors have occurred, they have always been ones of detail, procedure or human oversight rather than malicious intent. Any product obtained through such errors has been destroyed. When I receive reports of errors, these are always in-depth reports, drafted by senior management, with any changes to process which they suggest or I put forward incorporated into subsequent guidance or training programmes for staff.

**Communication Service Providers**

2.12 I have continued the practice as in previous years of making informal annual visits to the main communication service providers (CSPs). These meetings, not required by the legislation, are again reflective of the good relationship enjoyed between myself, the CSPs and the intelligence community. In 2010 I visited Royal Mail and other CSPs engaged in supporting security and law enforcement agencies with interception.

2.13 The purpose of these visits, many of which commonly take place out of London, has been for me to meet on an informal basis senior staff and individuals engaged in interception work on the ground, in order to be briefed on changes to technology and working relationships between the intercepting agencies and CSPs. The staff within CSPs welcome these visits and the opportunity to discuss with me their work, safeguards that they employ, issues of concern and their relationships with intercepting agencies. I have attempted where possible to resolve any difficulties that have arisen between the intercepting agencies and CSPs.

2.14 As with members of the agencies engaged in interception work, I believe that those small numbers of staff who work within this field in CSPs are committed, professional and have a detailed understanding of legislation and appropriate safeguards. They recognise the importance of the public interest and national security implications of their work and undertake it diligently and with significant levels of dedication.

# 3. DISCUSSING MY ROLE

3.1 I have taken the opportunity on a number of occasions over the last year to discuss, as far as I feel qualified to do so, my work as Interception of Communications Commissioner.

**IIRAC Sydney 2010**

3.2 Along with Sir Peter Gibson, then Intelligence Services Commissioner, I attended the seventh international biennial conference of the International Intelligence Review agencies in Sydney, Australia between 21st and 24th March 2010. The aim of the conference was to explore and exchange views on principles and practices underpinning international models of intelligence oversight. Issues explored ranged from assurances of effective review of respective agencies' conduct to whether or not oversight should be retrospective or focussed on current operations.

3.3 I was asked and gladly agreed to lead a breakout session on the issue of effective review. My session discussed specifically *'Lawyers representing targets of national security interest: legal professional privilege and formal representation of their clients;* I found the discussion of such pertinent issues with colleagues from countries as diverse as Belgium, South Africa, New Zealand, Canada, Poland and the USA interesting, informative and valuable.

3.4 I was accompanied on this visit by members of the Intelligence and Security Committee (ISC). Sir Peter Gibson and I were unable to meet that committee in London in 2010 as we had done in previous years, due to the General Election. I found it valuable to engage with members of the ISC during this visit on areas of mutual interest.

**RUSI conference**

3.5 On the 24th November 2010, I accepted an invitation from the Royal United Services Institute, an independent defence think-tank, to contribute to a discussion on Intelligence oversight. The event was attended by security officials, academics and a small number of Parliamentarians with an interest in intelligence oversight. I gave a largely factual account during this event of my role as Interception Commissioner, detailing the relevant legislation, my oversight function as defined therein in addition to some of the risks, challenges and benefits inherent within interception. I found the opportunity to discuss my role within the intelligence oversight framework enjoyable and beneficial.

# 4. STATISTICS

**Figure 4: Home Secretary and Scottish Government warrants extant, issued and modifications between 2008 and 2010**

| | Warrants in force 31st Dec | | | Warrants issued in year | | |
|---|---|---|---|---|---|---|
| | 2010 | 2009 | 2008 | 2010 | 2009 | 2008 |
| **Home Secretary** | 1048 | 959 | 844 | 1682 | 1514 | 1508 |
| | Senior official | | | | | |
| **Number of modified in year** | 5761 | 5267 | 5344 | | | |
| | 2010 | 2009 | 2008 | 2010 | 2009 | 2008 |
| **Scottish Government** | 46 | 69 | 43 | 183 | 192 | 204 |
| **Number of modifications in year** | 648 | 629 | 610 | | | |

4.1 In previous annual reports I have considered at this stage the number of errors reported to me by intercepting agencies. This year, I believe it would add context for the error reports that follow for the reader to be made aware of trends in the total number of interception warrants issued and modified by those Secretaries of State, namely the Home Secretary and Scottish Ministers, whose figures have previously been released in the open version of my report.

4.2 As illustrated in Figures 4 to 6, the total number of warrants authorised by the Home Secretary in-year has increased from 1508 in 2008 to 1682 in 2010, whereas the number of warrants issued by the Scottish Ministers over the same period has fallen from 204 to 183. These changes represent percentage increases of 10% and decreases of 10% respectively in the number of warrants signed. In addition, the number of warrants extant at year-end has increased from 844 in 2008 to 1048 in relation to the Home Secretary and from 43 to 46 in relation to Scottish Ministers. Again, these figures represent increases of 20% and 5% respectively

**Figure 5: Number of Home Secretary and Scottish Government warrants in force at year-end**

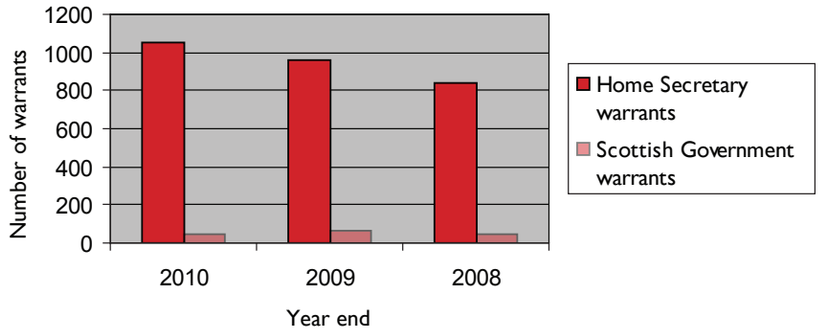
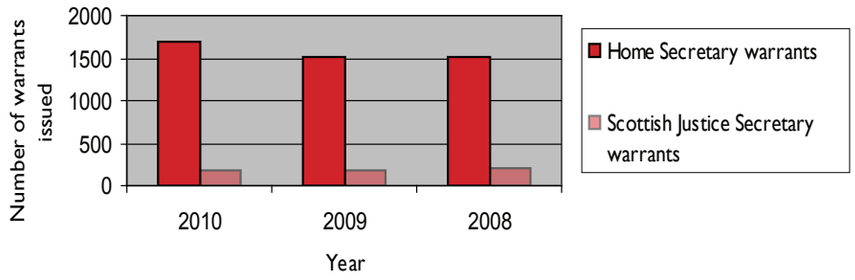



**Figure 6: Number of Home Secretary and Scottish Government warrants issued in year**




4.3 The increases in both extant and in-year warrant numbers between 2008 and 2010 show that the UK faces significant and growing problems arising from serious crime, and threats to national security. Interception is being used increasingly to counter such threats. It is also impressive to see how interception has contributed to a number of significant law enforcement successes, as detailed in the next section.

4.4 Readers may also be aware that both the Foreign Secretary and the Secretary of State for Northern Ireland authorise applications for interception warrants. I have decided to continue with the practice of previous years in not disclosing details of the numbers of such warrants in the open section of my report. This is because I remain convinced that the disclosure of Home Secretary warrants does not provide hostile agencies with any indications of targets as the total number includes both warrants issued in the interest of national security and for the prevention and detection of serious crime. In the case of Scottish Government warrants, the numbers disclosed represent the total number of serious crime warrants. In the case of Foreign Office and Northern Ireland warrants, however, I believe it is prejudicial to national security to disclose warrantry statistics outside of the Confidential Annex as it may enable hostile agencies to estimate even approximately the extent to which any interception of communications was being undertaken to protect national security.

# 5. SUCCESSES

5.1 I have been impressed to see how interception has contributed to a large number of significant law enforcement and national security successes during 2010, as in previous years. Interception is a powerful investigative tool for law enforcement agencies, including in operations to tackle large-scale drug trafficking, excise evasion, people trafficking and other serious crimes. Many of the most significant terrorist disruptions in the recent past have been aided by intelligence gathered through interception.

5.2 The SOCA case summary shown on this page represents merely one of a large number of operations that readers may have heard about in the national media where interception has played a role in a successful outcome. I have, as in previous years, in order not to prejudice national security, provided detailed examples of such operations in the Confidential Annex of this report. Readers must be aware that interception cannot be used in isolation; it is part of a range of investigative techniques I have seen used by security and law enforcement agencies, but only when a case can be made that it is necessary and proportionate to do so. Although huge intelligence and investigative benefits can be reaped from interception, it has the potential to be a highly intrusive tool. That is why the tests of necessity and proportionality outlined in RIPA and the scrutiny provided by myself, my Inspectors and others tasked with intelligence oversight are crucial.

SOCA Case study

This report concerns a SOCA investigation undertaken between 2009 and 2010. The details have been sanitized in order to prevent association with a specific operation. Originating from a seizure of a substantial consignment of Class A controlled drugs by the UK overseas law enforcement partners, members of a UK based organised crime group (OCG) were identified as recipients of the consignment. SOCA assessed that it was necessary and proportionate for two senior members of the OCG to be subjects of an intercept led operation.

The operation commenced in mid-2009, intercept intelligence immediately identified a number of members of this OCG, allowing a better understanding of the way in which this OCG operated.

Intelligence gained from interception enabled SOCA to coordinate the arrest of one of the principle members of this OCG and a criminal associate in connection with the seizure of in excess of 25 kg of Class A controlled drugs. Despite these arrests and seizure, the remaining principal of the OCG continued to coordinate the supply and distribution of controlled drugs, and as a result of this the collection of intercept intelligence continued.

Intercept intelligence provided an opportunity to arrest this subject and two members of the OCG which had supplied in excess of 20kg of class B drugs. All three were charged with drugs offences.

*Continued*

It was also identified through interception that two members of the OCG had been tasked with organising the murder of an unidentified individual who owed a substantial amount of money for previously supplied consignments of controlled drugs. Subsequent intercept intelligence identified the individual tasked with conducting this murder. As a result of intercept intelligence three people were arrested and charged with conspiracy to murder.

It is conservatively estimated that an investigation into a murder costs an ACPO force approximately £1million. In this case the targeting, by use of interception, of those involved in conspiring to murder an individual over a drugs debt has had an identifiable saving to the public purse.

Overall this interception-led operation lasted less than 12 months and during that period interception intelligence enabled actionable evidence to be gathered which has had a significant impact on the activities of this OCG, both in the UK and abroad.

In total more than 15 persons associated with the OCG have been arrested for offences of supply and distribution of controlled drugs, money laundering, possession of firearms and conspiracy to murder.

In excess of 300 kilograms of controlled drugs have been seized, the majority of which has been Class A. Approximately £750,000 has been seized along with a number of firearms.

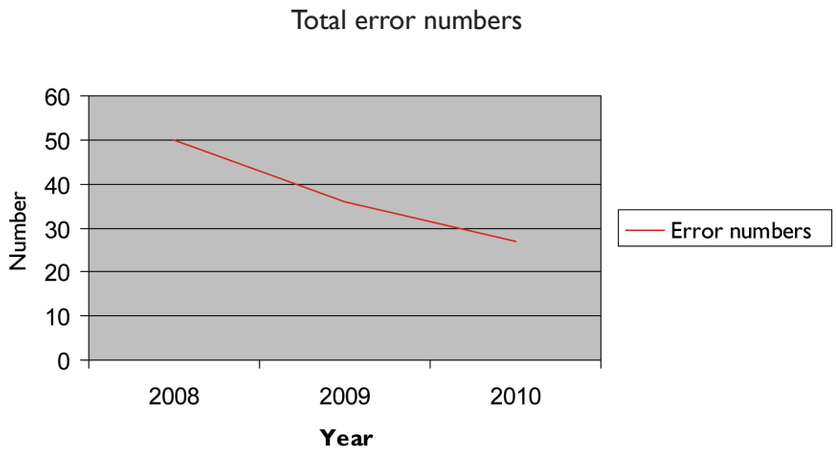
Intercept intelligence gathered has increased the understanding of how this and other OCGs operate, including how they negotiate and interact with other OCGs. During the course of this operation actionable intelligence was disseminated by SOCA to ACPO forces and European law enforcement partners.

Of the 7 individuals subject to interception of their communications 5 have been prosecuted with 4 receiving significant sentences which total in excess of 20 years. One individual is still awaiting sentencing. Of the two who were not arrested or charged they have both in the short term ceased their significant criminal activity with one departing the UK.

This operation was subject to inspection during the reporting year 2009/10.

# 6. ERRORS

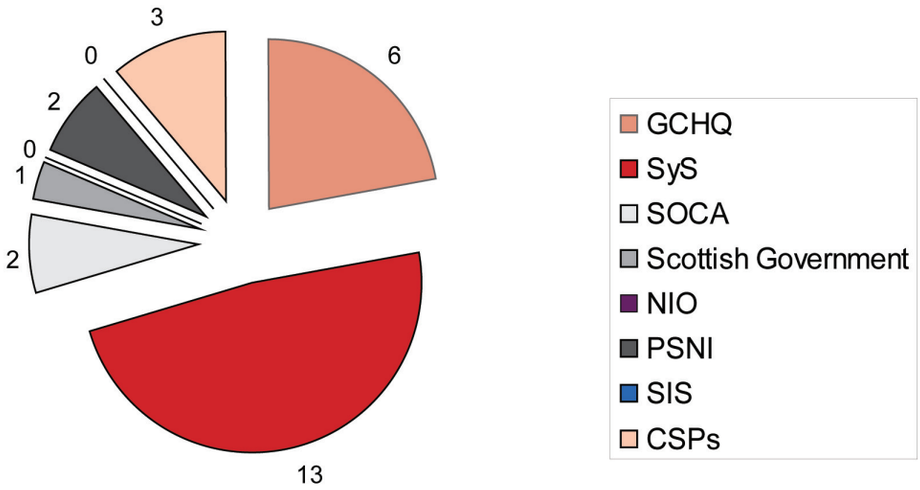
**Figure 7 Year on year changes in total error numbers between 2008 and 2010**




6.1 Twenty seven errors have been reported to me during the course of 2010. This represents a 25% decrease on the 36 errors reported in 2009, and furthermore an approximately 46% decrease in the 50 errors reported in 2008. As in previous years, full details of these errors are contained in the Confidential Annex of the current report. However, I hope that readers will draw confidence from the broad details of errors contained in the summary table contained in Figure 10.

6.2 It is important to note that none of the reported errors or breaches were deliberate. All were caused, as reported in previous years, by human or procedural error, technical problems or through the testing of prototype systems. In every case either no interception took place, or, if any interception did occur, the product was destroyed. Readers should note that where breaches or errors do occur, systems are revised or strengthened, guidance is issued or training initiated to minimise the risks of similar mistakes being repeated in future.

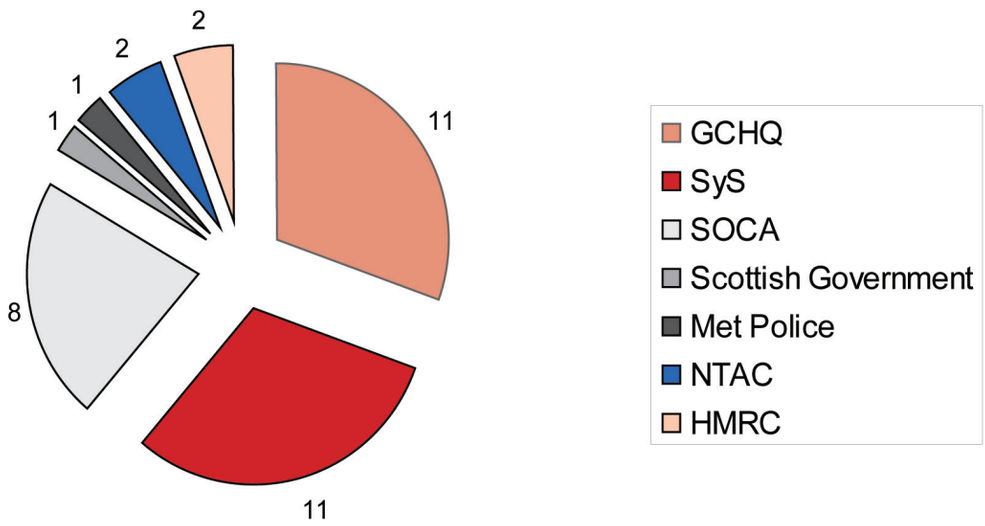
**Figure 8: Number interception errors broken down by Agency in 2010**




Home Office/SIS/MoD/Met Police/HMRC/NIO and NTAC reported no errors in 2010

6.3 Based on useful past feedback I have attempted in this year's annual report to give, as far as I am able to without being prejudicial to national security, more details of the kinds of errors reported to me by intercepting agencies. Figure 10 is the product of this approach. Readers will be aware from the information presented thus far that the Secret Intelligence Service, Northern Ireland Office, Home Office, Ministry of Defence, Metropolitan Police Counter-Terrorism Command, Her Majesty's Revenue and Customs and the National Technical Assistance Centre reported no errors during 2010. There remain, however, certain errors details of which I am unable to give without prejudicing safeguards protecting national security and the modus operandi of our law enforcement and intelligence agencies. Therefore, some of the generic examples I outline in the grid are typical of the whole and are anonymous so far as the targets are concerned.

**Figure 9: Number interception errors broken down by Agency in 2009**




SIS/NIO/PSNI/Home Office/MoD and CSPs reported no errors in 2009

6.4 It is also worth noting that sometimes a single mistake by an operator (e.g. the failure to apply a specific filter to material being gathered for examination) can result in a large number of errors. In such cases, each item gathered, which would not have been gathered had the filter been properly applied, counts as an error. In these cases, for the purpose of comparison it is more sensible to treat the mistake as one error.

**Figure 10 : Details of selected interception errors**

| Agency | Total number of errors | Date/ periods of errors | Selected details of errors |
|---|---|---|---|
| **GCHQ** | 6 | Early 2010 | Error 1 was identified during a routine system check and resulted from forwarding collected material based on out-of-date selectors from a particular interception system. It was caused by human error. Relevant teams have been made aware of specific risks involved when changing forwarding arrangements. Migration to new selector management systems has ensured that this particular error will not recur. |
| | | February | Error 2 involved a failure to remove selectors from a range of interception systems even though steps had been taken to cease collection against the associated targets. This was due to complex technical system issues. A thorough investigation was undertaken by collection management staff, with considerable resource applied. A number of mitigating measures were implemented prior to a major system re-design. |
| | | March | Error 3 concerned a scenario where there was rapid tasking and de-tasking of the same selectors to/from certain interception systems. Due to two separate software bugs, selectors were not properly de-tasked when this particular scenario occurred. Once the error had been investigated, all erroneously collected material was deleted and a new version of software fixed the bugs. Communications between software engineers and collection management staff have also been improved. |

| | | | |
|---|---|---|---|
| | | April | Error 4 refers to the failure to remove a specific filter to material being gathered for examination, which resulted in intercept product being collected after the warrant (s) had lapsed or been cancelled. A thorough investigation of the circumstances surrounding this unauthorised interception and general practice to date was conducted by the agency in consultation with the Home Office. Errors had occurred due to a lack of communication between various investigatory, warrantry and technical sections alongside a broader lack of understanding of warrantry requirements. A number of steps have been reported to ensure greater rigour is applied to filtering material so that similar errors are avoided in future. This has involved another level of governance and internal oversight being implemented, alongside greater collaboration between different sections across the Agency.Future training programmes will incorporate these changes. |
| | | July | Error 5 related to the pilot phase of a prototype collection system. Particular technical conditions that had not been foreseen resulted in over-collection of data. Once discovered, all erroneously collected data was purged from the system. New technical rules and checks were put in place for future iterations of the system. The lessons learned from this incident were disseminated to technical development teams to inform future development work |
| | | September | Error 6 was identified during a routine sampling check and concerned inconsistency between a specific warrantry schedule and the subsequent targeting of systems. It was due to human error. Once the inconsistency was identified, all relevant intercepted material was deleted. New safeguards to address this issue have been introduced, including extra briefing and training, the provision of regular summaries of warranted selectors, and an explanation of individual roles and responsibilities in relation to the warrantry process. |
| Security Service | 13 | | I include details of four different kinds of errors directly attributable to the Security Service |
| | | January | Error 1 was related to an oversight by the Service in relation to differing forms of communications warranted under a specific schedule. The error was picked up through a query from another Department and once the error was identified interception was immediately suspended. The error has lead to a reassessment of specific forms of communications and their authorisation on warrantry paperwork and associated schedules. |

| | | | |
|---|---|---|---|
| | | January | Errors 2 and 3 involved warrants where an incorrect digit was used when warrantry paperwork was completed, due to human error. This resulted in incorrect phone numbers being intercepted. Where in one case product was collected, the interception was immediately cancelled and all product destroyed. On each occasion the officer involved was briefed again on the importance of accuracy and cross-checking when completing warrantry applications. |
| | | July | Error 4 refers to the failure to remove a specific filter to material being gathered for examination, which resulted in intercept product being collected after the warrant (s) had lapsed or been cancelled. A thorough investigation of the circumstances surrounding this unauthorised interception and general practice to date was conducted by the agency in consultation with the Home Office. Errors had occurred due to a lack of communication between various investigatory, warrantry and technical sections alongside a broader lack of understanding of warrantry requirements. A number of steps have been reported to ensure greater rigour is applied to filtering classes of material so that similar errors are avoided in future. This has involved another level of governance and internal oversight being implemented, alongside greater collaboration between different sections across the agency. Filtering will also be considered discretely in future training programmes. |
| | | Sept | Error 5 refers to unauthorised interception of product related to a communications address that had not been properly assessed as belonging to a target. A specific method was used to attempt to obtain target communication addresses which later turned out to have picked up an incorrect address. A warrant was applied for and interception commenced on this address. The error was not picked up due to automated intercept collection systems. Once human intervention had revealed the error, the interception was stopped and a number of changes introduced with specific assessment being made after a period of time to confirm the veracity of communications addresses. |

| | | | |
|---|---|---|---|
| **SOCA** | 2 | May | Error 1 involved the incorrect transposition of a target telephone number from a warrantry certificate. Subsequent feasibility checks between the intercepting agency and the CSP did not pick up the error in transposition, thus leading to an incorrect number being intercepted. Once it was noted that the user of the telephone was not the target, a fault report was made to technical department and the line suspended. All product was immediately destroyed. Both SOCA technical collection department and the relevant CSP managers were reminded of the importance of cross-checking telephone numbers at various feasibility stages and of wider responsibilities in such matters. |
| | | August | Error 2 involved the incorrect modification and subsequent interception of a telephone number in a rapidly moving operation. An officer incorrectly voice-matched a target to a phone number, which was subsequently activated for interception. Once the error was realised, all interception was suspended and product immediately destroyed. As an outcome all officers were reminded of the need to be as confident as possible as to target communications addresses when applying for modifications to warrants. Officers have been reminded of the need to seek corroborating intelligence before making such applications for amendments. It was accepted that this may be difficult during particularly time-critical and life-threatening operations. |
| Police Service Northern Ireland | 2 | February and April 2010 | Both errors reported to me by PSNI were concerned with simple human error, namely the incorrect transposition of a communications address between in the first case a reliable Covert Human Intelligence Source (CHIS) and the agency, and in the second case between PSNI and another public authority. In both cases checks had been unable to pick up the error, however once it was discovered, interception was immediately ceased and all product destroyed. PSNI have re-emphasized to staff working in this area to check the accuracy of their information with as many sources as possible before applying for warrants and beginning interception. |

| | | | |
|---|---|---|---|
| Scottish Government | 1 | November | The single error arising from a Scottish Government warrant relates to a breach of interception by a Scottish Police Force. An application was made to modify an interception warrant but it transpired that neither of the telephone numbers placed under intercept warrants were being used by the target. This was due to police force misinterpretation of intelligence. Once discovered to be incorrect, interception on the communications addresses was immediately suspended and product destroyed. The police force subsequently revised its internal procedures to reduce the likelihood of a repeat of a similar error in the future. |
| Communications Service Providers | 3 | July | Error 1 relates to a human error by a member of CSP staff, whereby a feasibility call was conducted on an agency contact officer's number rather than the warranted target number. Therefore the incorrect transposition of a phone number led to the wrong mobile telephone being placed under intercept. Staff changes and weekend leave meant that the error was not uncovered until three days after interception commenced. Once the error was understood interception was immediately suspended and any product collected was destroyed. The CSP reviewed the incident and implemented a new pro-forma which separated warranty details from contact details to ensure such a mistake was not repeated in future. |
| | | November | Error 2 involved the incorrect transposition of a communications address at feasibility stage into a targeting database, thus leading to unintended interception of an individual's communications. The error was not picked up at a subsequent level of cross-checking and thus once the agency reported that the product was likely to be breach data the line was immediately suspended and all product immediately destroyed. The breach was due to human error. The CSP implemented changes that involve engineers crosschecking communications addresses with customer records at the signing stage to ensure such a mistake is not repeated in future. |

# 7: PART I CHAPTER II OF RIPA

## Acquisition and Disclosure of Communications Data

### General Background

7.1 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, under Chapter II of Part I of RIPA, to assist them in carrying out their investigatory or intelligence function. They include the intelligence agencies, police forces, the United Kingdom Border Agency (UKBA), the Serious Organised Crime Agency (SOCA) and other public authorities such as the Gambling Commission, Financial Services Authority (FSA) and Local Authorities.

7.2 Any access to communications data by public authorities is an intrusion into someone's privacy. To be justified, such intrusion must satisfy the principles of necessity and proportionality derived from the European Convention on Human Rights (ECHR) and embedded in RIPA. 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. The Act and its Code of Practice contain explicit human rights safeguards. These include restrictions, prescribed by Parliament, on the statutory purposes for which public authorities may acquire data; on the type of data public authorities may acquire; which senior officials within public authorities may exercise the power to obtain data; and which individuals within public authorities undertake the work to acquire the data.

7.3 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. 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 public authorities understand that I oversee the use of their powers and I believe that it is in the public interest that public authorities should demonstrate that they make lawful and effective use of their powers.

### Inspection Regime

7.4 The acquisition of communications data generally involves four roles within a public authority; the Applicant who is the person involved in conducting an investigation who submits the application for communications data, the Designated Person (DP) who objectively and independently considers and authorises the application, the Single Point of Contact (SPoC) who is an accredited individual responsible for acquiring the data from the Communication Service Provider (CSP) and ensuring that the public authority acts in an informed and lawful manner; and the Senior Responsible Officer (SRO) who is responsible for the overall integrity of the process. Adherence to the Act and Code of Practice by public authorities 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 the incorrect data being disclosed.

7.5 The primary objectives of the inspections are to:

- Ensure that the systems in place for acquiring communications data are sufficient for the purposes of the Act and that all relevant records have been kept.
- Ensure that all acquisition of communications data has been carried out lawfully and in accordance with Chapter II of Part 1 of RIPA and its associated Code of Practice.
- Provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct authorised.
- Examine what use has been made of the communications data acquired to ascertain whether it has been used to good effect.
- Ensure that errors are being 'reported' or 'recorded' and that the systems are reviewed and adapted where any weaknesses or faults are exposed.
- Ensure that persons engaged in the acquisition of communications data are adequately trained.

7.6 At the start of the inspections my Inspectors review any action points and recommendations from the previous inspection to check they have been implemented. The systems and procedures in place for acquiring communications data within the public authority are examined to check they are fit for purpose.

7.7 My Inspectors carry out an examination of the communications data applications submitted by the public authority. It is difficult to set a target figure for the number of applications that are examined in each public authority as the volume will obviously vary significantly depending on the public authority being inspected. Where the public authority has only submitted a small number of applications it is likely that they will all be examined. However for the larger users, a random sample is selected which embraces all of the types of communications data the particular public authority is permitted to acquire.

7.8 My Inspectors seek to ensure that the communications data was acquired for the correct purpose as set out in Section 22(2) of RIPA and that the disclosure required was necessary and proportionate to the task in hand. The Inspectors assess the guardian and gatekeeper function being performed by the SPoC against the responsibilities outlined in the Code of Practice. A range of applications that have been submitted by different applicants and considered by different DPs are examined to ensure that there is uniformity in the standards and that the appropriate levels of authority have been obtained. My Inspectors scrutinise the quality of the DPs considerations and the content of any authorisations granted and / or notices issued.

7.9 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. The CSPs are asked to provide my Inspectors with details of the communications data they have disclosed to the public authorities during a specified period. The disclosures are randomly checked against the records kept by the public authorities in order to verify that documentation is available to support the acquisition of the data.

7.10 My Inspectors conduct informal interviews with senior investigating officers, applicants and analysts to examine what use has been made of the communications data acquired and to ascertain whether it has been used to good effect. During this part of the inspection if necessary they will, and often do, challenge the justifications for acquiring the data. Later in my report I will highlight a few examples of how communications data has been used effectively by public authorities to investigate criminal offences.

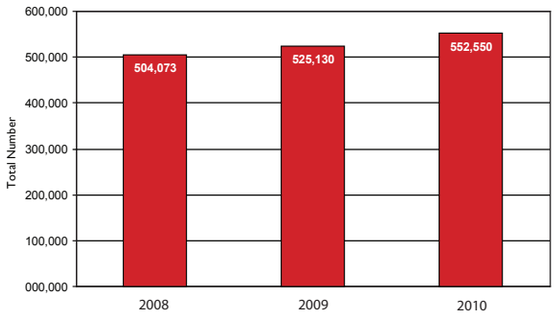
7.11 Any errors which have already been reported or recorded are scrutinised to check that there are no inherent failings in the systems and procedures and that action has been taken to prevent recurrence.

7.12 Following each inspection a detailed report is prepared and this outlines inter alia what level of compliance has been achieved with the Act and Code of Practice. I have sight of all of the inspection reports in order to discharge properly my oversight functions. Where necessary, an action plan will accompany the report which specifies the areas that require remedial action. A copy of the report is sent to the head of the public authority concerned, e.g., the Chief Constable in the case of a police force or the Chief Executive in the case of a local authority. They are required to confirm, within a prescribed time period, that the recommendations have been implemented or outline the progress they have made to achieve the recommendations.

**Communications Data Statistics**

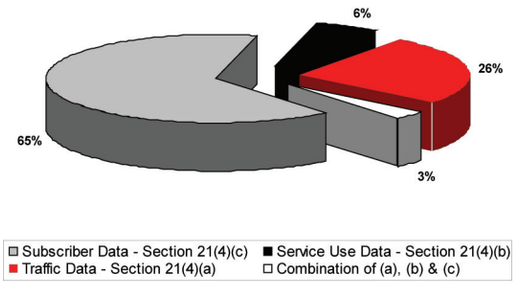
7.13 During the reporting year public authorities as a whole, submitted 552,550 requests for communications data. The intelligence agencies, police forces and other law enforcement agencies are the principal users of communications data. Chart 1 illustrates that the number of requests submitted in the last three years has increased year on year by approximately 5%. I cannot give a precise reason for the steady increase, but it is indicative of the growth in communications technology. The statistics show that certain police forces have increased their demands for communications data and I believe that this is due, in part, to the fact that there is an increasing awareness amongst investigators of the type of communications data that is available and how communications data can used as powerful investigative tool.

Chart 1: Number of Notices / Authorisations for Communications Data in the previous three year period




7.14 Chart 2 illustrates the breakdown of the communications data requests by type. Nearly two thirds of the requests for communications data in the reporting year were for subscriber data under Section 21(4)(c), usually in the form of enquiries to ascertain the ownership of mobile phones.

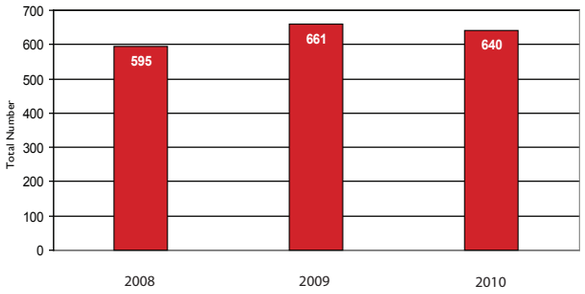
Chart 2: Percentage of Communications Data Requests by Type




7.15 During the reporting year, 640 errors were reported to my office by public authorities. This figure is slightly less than the previous year; however it does not take account of an additional 1061 errors also reported to my office in 2010. I have kept these additional errors separate from the overall figure as they are unusual in that they were all reported by one public authority. These additional 1061 errors were caused by two separate technical faults in that public authority's systems and are discussed in the Intelligence agencies section of this report. It is also worth noting that sometimes a single mistake by an operator (e.g. the failure to apply a specific filter to material being gathered for examination) can result in a large number of errors. In such cases, each item gathered, which would not have been gathered had the filter been properly applied,

counts theoretically as an error. In these cases, however, for the purpose of comparison it is more sensible to treat the mistake as one error. Overall however the error rate is still low and indeed minute (0.3%) when compared to the number of requests that were made by all public authorities during the course of the reporting year.

Chart 3: Number of Errors Reported to the Commissioner in the previous three year period




7.16 Approximately 82% of the 640 errors were attributable to public authorities and the remaining 18% to CSPs. A considerable proportion of these errors were due to the incorrect transposition of telephone numbers or dates. More police forces and CSPs are introducing automated systems to manage their requirements for communications data and these will reduce the number of keying errors which occur. It is inevitable that some mistakes will be made, especially when public authorities are dealing with large volumes of communications data in complex investigations.

7.17 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 public authority understands that it must strive to achieve the highest possible standards.

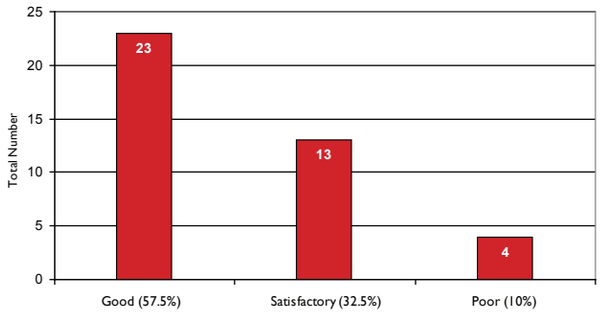
## Review of 2010 Communications Data Inspections

### Police Forces and Law Enforcement Agencies

7.18 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; Ministry of Defence Police; Royal Navy Police and the Civil Nuclear Constabulary. Law enforcement agencies comprise Her Majesty's Revenue and Customs (HMRC); the Serious Organised Crime Agency (SOCA); the Scottish Crime and Drug Enforcement Agency (SCDEA); United Kingdom Border Agency (UKBA); and the Child Exploitation & Online Protection Centre (CEOP).

7.19 In 2010 my inspection team conducted 40 inspections of police forces and law enforcement agencies. 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. Chart 4 illustrates that 90% of the police forces and law enforcement agencies achieved a good or satisfactory level of compliance overall.

Chart 4: Law Enforcement Agency Inspection Results 2010




7.20 My Inspectors found that the vast majority of police forces and law enforcement agencies had fully implemented their previous recommendations. As a consequence an overwhelming number have either improved or sustained their good level of compliance with the Act and Code of Practice. Conversely, those that emerged poorly from the inspections had all been slow to respond to the findings from their previous inspections and had not implemented all of their recommendations. I have now been provided with assurances by these police forces and law enforcement agencies that they are working towards achieving their recommendations, if they have not already achieved them. Nevertheless, these police forces and law enforcement agencies will be subject to earlier re-inspections to check that they have improved their standards.

7.21 Three of the four police forces and law enforcement agencies that emerged poorly from their inspections did not have sufficient trained staff in their SPoC. The SPoC has an important responsibility under the Code of Practice to make sure the public authority acts in an informed and lawful manner and therefore it is vitally important for public authorities to have the right number of well trained staff in this business area. It is vital for the systems and procedures to be maintained in the most efficient and effective manner and more often than not this also relies on having the right number of well trained staff. A lack of staff often results in serious backlogs in the applications and where this occurs there is a risk that applicants will be hindered from achieving their investigative objectives because the data is not getting to them quickly enough. The impact of this upon investigations is incalculable. My Inspectors have recommended that these police forces and law enforcement agencies should take the necessary steps to ensure that they have sufficient trained staff in their SPoC.

7.22 94% of the police forces and law enforcement agencies that were inspected during the reporting year were consistently producing good or satisfactory quality applications. The remaining 6% were producing applications to an inconsistent standard. In these cases, advice has been provided to assist the applicants to improve the overall quality of their applications and the SPoCs have also been encouraged to take a more robust guardian and gatekeeper function in this respect. In my last annual report I commented that it was disappointing to find that almost half of the police forces and law enforcement agencies inspected had taken little or no advantage of the streamlining procedures which were introduced when the Code of Practice was approved by Parliament in October 2007. I am pleased to report that virtually all of those inspected in this reporting year had introduced the streamlining procedures and these have improved the efficiency and effectiveness of the process and reduced bureaucracy, without undermining the rigour of the process.

7.23 The inspections identified that over a third of the police forces and law enforcement agencies had amended the questions and / or guidance prompts on the Home Office and ACPO Data Communications Group (DCG) application form template. As a result their application processes were unnecessarily complicated, repetitive and bureaucratic. This was disappointing and my Inspectors have urged these police forces and law enforcement agencies to realign their application forms to the national template. This will make the applications more focused and succinct and raise the standard across the board.

7.24 A number of CSP disclosures were randomly checked against the records kept by the police forces and law enforcement agencies and 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 DP. 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 unlawful acquisition of communications data.

7.25 My Inspectors concluded that the DPs are generally discharging their statutory duties responsibly. The DPs in 65% of the police forces and law enforcement agencies were found to be recording their considerations to a consistently good standard. It was quite clear that these DPs were individually assessing each application, taking on board the advice provided by the SPoC and questioning the necessity and proportionality of the proposed conduct. In the remaining police forces and law enforcement agencies inconsistencies were evident in the standards being achieved. Furthermore, my Inspectors were concerned to find that in 2 police forces a number of the DPs had not actually recorded any written considerations when approving some of the applications and this constitutes non-compliance with Paragraph 3.7 of the Code of Practice. In both of these cases the DPs had mistakenly believed that they did not need to record any considerations due to a misunderstanding in relation to how to use their respective authority's application system. In another police force a number of different DPs were found to be sharing the same set of identical considerations which is poor practice. It is vitally important for DPs to ensure that they are writing their own considerations as this will provide evidence that each application has been duly considered. Evidently there are training and quality assurance issues to resolve in relation to the DPs in some of the police forces and law enforcement agencies.

7.26 Generally a good level of independence and objectivity exists in the DP approvals process. The exception to this was in relation to some of the applications submitted by specialist departments, namely Special Branch (SB) and Professional Standards (PSD), where my Inspectors had concerns that Paragraph 3.11 of the Code of Practice was not always being complied with. Due to the sensitive nature of the work undertaken by SB and PSD it is accepted that on occasions, for reasons of security, a person who is directly involved in an investigation may need to act as the DP. This is permissible, but the Code of Practice outlines that where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of the DP must be explicit in their recorded considerations. This requirement must be complied with.

7.27 Communications data can only be acquired by PSD for the purpose of preventing and detecting crime and therefore cannot be acquired in relation to misconduct or disciplinary investigations where there is no intention to conduct a criminal investigation. During the reporting year one police force reported an error to my office where communications data had been acquired in relation to a disciplinary investigation and this is a positive indication that public authorities are self auditing and identifying any conduct which constitutes non-compliance. Two further errors of this type were identified by my Inspectors during their inspection of another police force, and both of these errors related to the same investigation. The police forces concerned have confirmed that the communications data that was acquired will not be used in the misconduct / disciplinary investigations and have provided a reassurance that they have put measures in place to prevent recurrence of similar errors.

7.28 The urgent oral process is principally used to acquire communications data when there are immediate threats to life and usually this applies when vulnerable or suicidal persons are reported missing, in connection with abduction or kidnap situations or in relation to other crimes involving serious violence. This is an important facility, particularly for police forces, and the interaction between the SPoCs and the CSPs saves lives across the country on a continuous basis. Good use is also being made of the urgent oral process where there is an exceptionally urgent operational requirement, and where the data will directly assist the prevention or detection of a serious crime, the making of arrests, or the seizure of illicit material. In the reporting year 31,210 requests were orally approved which represents a significant increase on last year's figure of 21,582. I am aware that a number of police force SPoCs are now supporting serious crime investigations out of office hours where previously they only had the resources to support immediate threats to life. Furthermore a small number of SPoCs have started to operate on a 24/7 basis. Both of these facts may account for some or all of the increase. Again marked improvements were found in the management of the urgent oral process and the quality of the record keeping with 87% of the police forces and law enforcement agencies now achieving a good or satisfactory standard in this area.

7.29 During the reporting year some of the police forces have started to take advantage of the collaboration provisions in the Policing and Crime Act 2009, particularly to support the out of office hours requests. It is likely that in the future more police forces will brigade their SPoC resources into a region and my Inspection timetable will reflect any such collaborative arrangements.

7.30 It is evident that police forces and law enforcement agencies are making good use of communications data as a powerful investigative tool, primarily to prevent and detect 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. SPoCs throughout the UK continue to provide a valuable service to the investigation teams and often they make a significant contribution to the successful outcome of operations. I would like to highlight a few examples of how communications data is used by police forces and law enforcement agencies to investigate criminal offences as they may provide a better understanding of its importance to criminal investigations. The following three examples are based on extracts from the Inspector's reports.

**Case Study 1**
Cheshire Police – Operation Wood

Cheshire Police used communications data to very good effect when investigating an Organised Crime Group involved in the supply and distribution of Class A drugs. A range of communications data was acquired in relation to this case, including subscriber information, incoming and outgoing call data and cellsite data. The analysis of the data assisted to attribute the phones to individual members of the (OCG) and place them in specific areas when they were conspiring to source or supply drugs. This proved to be invaluable from an evidential perspective. One of the members of the OCG was only identified as a result of the acquisition of communications data. This individual was an accountant who was laundering the OCGs illicit cash and also dealing drugs himself. Ultimately 13 persons were charged with offences relating to the supply of Class A drugs. Cash to the value of £20,000 was seized during the operation together with 4kgs of cocaine. The weight of the communications data evidence was overwhelming and in June 2010 at Chester Crown Court all of the defendants pleaded guilty. They received sentences totalling 62 years.

**Case Study 2**
Metropolitan Police – Operation Gulpin

The Metropolitan Police used communications data to very good effect when investigating a forty million pound jewellery robbery which took place at a jewellers in Mayfair, Central London. Two males entered the jewellers asking to view a specific diamond ring; both then produced handguns and forced a member of staff to open the display cabinets. The suspects left the store taking a female hostage at gunpoint and shots were fired towards those giving chase. CCTV captured the suspects just prior to entering the jewellers and this indicated that one was using a mobile phone. A mobile phone was later recovered in an abandoned vehicle linked the offence. Subscriber, service use and traffic data acquired on this telephone identified the following:

- the professional makeup artist who had altered the suspects hair with wigs, altered their skin tones and their features using latex prosthetics,
- a car firm used to hire a getaway vehicle,
- a dress hire company used to ensure the suspects blended into their surroundings,
- the locations of the suspects and persons of interest at relevant times,
- an indication of pre-planning (reconnaissance of the premises)

The communications data acquired was crucial to the investigation. Three men were convicted of conspiracy to rob and received custodial sentences of 16 years. One man was convicted of conspiracy to rob, kidnap and possession of a firearm and received a custodial sentence of 23 years.

**Case Study 2**
Lancashire Constabulary – Operation Lace

Lancashire Constabulary used communications data very effectively when investigating the murders of Mr Abdullah Aziz Mohammed and his wife Ayesha Mohammed, and the attempted murder of their two children. The communications data initially identified two suspects who were shown to travel simultaneously into the vicinity of the offence location at the relevant time. This evidence was used to present the case to the CPS who agreed a charge of murder. However from the evidence available these two suspects could not have been responsible for setting the fire and further communications data acquired in relation to the two suspects actually assisted to exonerate them from the murders. Four further suspects from the London area were eventually identified. The communications data acquired in relation to these individuals was crucial to the case and the four defendants received life sentences for the murders of Mr. and Mrs. Mohammed and the attempted murder of their two children. The Mohammed family were never the intended victims and their house was targeted in error.

**Intelligence Agencies**

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

7.32 During the reporting year the Security Service was inspected. It is the largest user of all the intelligence agencies. The Security Service emerged fairly well from the inspection. My Inspectors were generally satisfied the Security Service is acquiring communications data lawfully and overall they are achieving a good level of compliance with the Act and Code of Practice. The applications are being completed to a good standard and the SPoC is ensuring the data is acquired in a timely manner.

7.33 In 2010 the Security Service reported 1061 errors to my office which can be split into two categories. First, subscriber data was acquired in relation to 134 incorrect telephone numbers. These errors were caused by a formatting fault on an electronic spreadsheet which altered the last three digits of each of the telephone numbers to '000'. These unfortunate errors were identified by the Security Service and duly reported, which is again a positive indication that public authorities are self auditing and identifying any conduct which constitutes non-compliance. A degree of unintended collateral intrusion occurred in relation to these 134 requests as the subscriber data acquired had no connection or relevance to any investigation or operation being undertaken by the Security Service. In line with paragraph 6.21 of the Code of Practice the Security Service has now destroyed this material. The technical fault on the spreadsheet has been rectified and all requests are also now checked manually before being sent to the CSPs which will reduce the potential for recurrence of such errors.

7.34 Second, Internet Protocol (IP) histories were acquired in relation to a number of IP addresses and unfortunately, due to an incorrect setting on the system used by the Security Service, this data was approved by DPs of insufficient rank / grade. IP histories constitute traffic data under Section 21(4)(a) and the prescribed officer to approve traffic data in the Service is a General Duties 3 (GD3). The system was set to route IP history requests to DPs of at least the rank / level below (i.e. a General Duties 4). These procedural errors were identified by my Inspectors during the inspection of the Security Service and this highlights the importance of my oversight. The Security Service undertook an immediate audit of their system and ascertained that communications data had been acquired in relation to 927 IP addresses that had been inappropriately approved by GD4 officers. This data was not obtained fully in accordance with the law and these errors were duly reported to my office. The Inspectors were satisfied that these errors had no bearing on the actual justifications for acquiring the data (i.e. the requests were necessary and proportionate) and furthermore, it is important to point out that no collateral intrusion occurred in relation to these requests. The Security Service has corrected the setting on their system and this should prevent recurrence of such errors.

7.35 It is inevitable that some mistakes will be made, especially considering the fact the Security Service is dealing with large volumes of communications data requests in complex investigations and that there is a degree of automation in the process. It is important to make the point that their error rate is still very low in comparison with the number of requests which are processed for communications data. I am satisfied with the measures that the Security Service has put in place to rectify these issues and these should prevent recurrence of such errors. It is clear to me that the Security Service is committed to achieving the best possible level of compliance with the Act and Code of Practice.

**Local Authorities**

7.36 There are over 400 local authorities throughout the UK approved by Parliament to acquire communications data under the provisions of the Act. They are restricted in relation to the type of communications data they can obtain. They are permitted to acquire subscriber data or service use data under Sections 21(4)(c) and (b) respectively, but they cannot acquire traffic data under Section 21(4)(a). I believe the extent to which local authorities use communications data should be placed in context and it is important to point out that local authorities may only use their powers where they have a clear statutory duty and responsibility to conduct a criminal investigation.

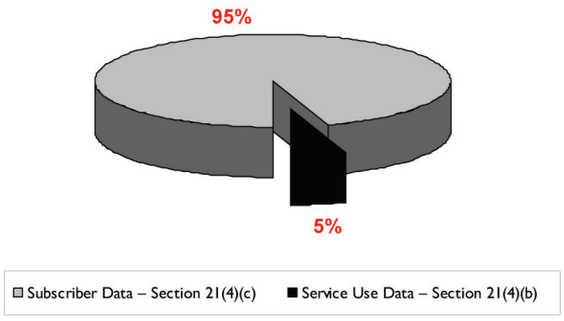
7.37 Generally the trading standards departments are the principal users of communications data within local authorities, although the environmental health departments and housing benefit fraud investigators also occasionally make use of the powers. Local authorities enforce numerous statutes and use 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.

7.38 Last year I reported that the Home Office funded the National Anti-Fraud Network (NAFN) 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 police counterparts. The first formal inspection of NAFN took place during the reporting period and I am pleased to report that it emerged extremely well. My Inspectors were satisfied that the communications data was being acquired lawfully and for the correct statutory purpose. The Accredited SPoCs at NAFN are providing an excellent service to their local authority members and are performing a robust guardian and gatekeeper function to ensure that the applications submitted by the different local authorities are completed to a consistently high standard. The NAFN SPoCs had also started to use their skills and expertise to engage proactively with applicants from the individual local authorities to ensure that the right data is obtained to meet the investigative objectives.

7.39 By comparison with police forces and law enforcement agencies, local authorities make very limited use of their powers to acquire communications data. During the period covered by this report 134 local authorities notified me they had made use of their powers to acquire communications data and between them they made a total of 1809 requests. This is a slight increase from the previous year's figures (131 local authorities, 1756 requests).

7.40 To put this figure into context, it represents just 0.3% of all communications data requests submitted by public authorities. 82% of the 134 local authorities made less than 20 requests in the reporting period and 60% made less than 10 requests. Chart 6 illustrates that 95% of the 1809 requests were for subscriber data under Section 21(4)(c) (i.e. name and address). Local authorities predominantly acquire subscriber data in order to identify the unknown suspect/s thought to be responsible for particular criminal offence/s. Only 22 of the 134 local authorities acquired service use data under Section 21(4)(b) and this accounted for the remaining 5% of requests. 34% of the 1809 requests were managed by the NAFN SPoC Service and this percentage is likely to increase in future as more local authorities sign up to the service.

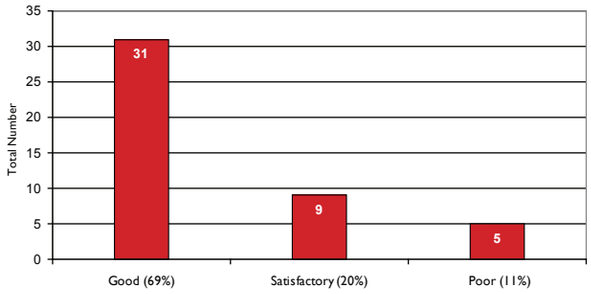
Chart 6: Local Authorities – Percentage of Communications Data Requests by Type




7.41 During the reporting year 26 inspections were conducted of individual local authorities. An additional 21 local authorities were inspected during the NAFN inspection which took place in July 2010 (although 2 of these had already been individually inspected). Therefore in total 45 inspections of local authorities were conducted. 19 of these local authorities were inspected for the first time, either because they had notified me that they had started to make use, or more frequent use, of their powers, or because they had used the NAFN SPoC service.

7.42 Chart 7 illustrates that 89% of the local authorities inspected achieved a good or satisfactory level of compliance with the Act and Code of Practice. These local authorities were completing their applications to a good standard and my Inspectors were satisfied that the DPs were discharging their statutory duties responsibly. My Inspectors found that in cases where communications data was required in relation to more than one telephone number or communications address, some applicants were needlessly submitting multiple applications when a composite one would have sufficed. Providing the telephone numbers or communications addresses are for the same investigation and that the source and the justification for acquiring the data in respect of all of the addresses is outlined, they should be submitted on one application as this reduces bureaucracy and improves the efficiency and effectiveness of the process.

Chart 7: Local Authority Inspection Results 2010 Chart 7: Local Authority Inspection Results 2010




7.43 Five of the local authorities did not emerge well from their inspections and serious failings and weaknesses were found in their systems and processes. The applications submitted by four of these public authorities lacked detail and on their own did not adequately justify the principles of necessity and proportionality. However, my Inspectors discussed the investigations with the relevant staff and concluded that the acquisition of the data was justified, nevertheless it is an established principle that an application for communications data should stand on its own and sufficient information must be included to enable the DP to make a decision whether the request is necessary and proportionate. In these cases it was apparent that the DPs were not basing their considerations on the basis of information outlined in the applications alone.

7.44 A few of the local authorities were not aware that it is the statutory duty of the DP to issue Section 22(4) Notices and the SPoCs were completing the Notices after the DPs had approved the applications. As a result procedural ('recordable') errors occurred, but importantly these had no bearings on the actual justifications for acquiring the data. In one local authority a number of the Section 22(4) Notices did not appropriately describe the communications data requested and as a result the CSPs misunderstood the requirements and disclosed outgoing call data under Section 21(4)(b) when in fact only subscriber data under Section 21(4)(c) had been requested by the applicant and approved by the DP. These instances constituted reportable errors and

have duly been reported to my office. Furthermore two local authorities reported two CSP errors to my office which occurred when the CSPs incorrectly disclosed traffic data under Section 21(4)(a) to the local authorities.

7.45 I am pleased to report that the local authorities all responded very positively to their inspections and I have been provided with assurances that the recommendations from their inspections have been implemented. Three of the five local authorities that emerged poorly from their inspections are now using the NAFN SPoC to manage their communications data requests and as a result they are now achieving a very good level of compliance with the Act and Code of Practice. The remaining two local authorities will be subject to an early re-inspection to check that they have improved their standards.

7.46 I am aware that some sections of the media have been very critical of local authorities in the past and there are allegations that they often use the powers which are conferred upon them under RIPA inappropriately. During the reporting year the applications examined by my Inspectors were all submitted in relation to investigations where local authorities have a clear statutory duty and responsibility to conduct a criminal investigation. My Inspectors looked at the use which local authorities had made of the communications data acquired 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 investigate the types of criminal offences which cause harm to the public, and many of which, if communications data were not available, would be impossible to investigate and would therefore go unpunished. I would like to highlight a few examples of how communications data is used by local authorities as this may provide a better understanding of its importance to the criminal investigations that local authorities undertake. Again, the following two examples are based on extracts from the Inspector's reports.

**Case Study 4**
Tower Hamlets London Borough Council – Fly-tipping

A prolific fly-tipper illegally dumped used car and motorbike tyres, instead of lawfully disposing of them in and around the Tower Hamlets and Newham areas of London. He chose industrial areas such as those in Bow and Stratford, near the Olympic Park construction site. Investigations revealed that he also fly-tipped across various other locations in London. Fly tipping allowed the individual to undercut lawful business and gained him sizeable financial rewards. In addition it fell to the affected London Boroughs to pay for the collection and disposal of the fly-tipped tyres. Illegal tyre dumping costs the tax payer around £2m a year to clear up, not to mention the environmental risk of fire and pollution. Subject to where the dumping occurs it can mean that facilities provided for the benefit of the public cannot be used, highways can be blocked and waterways, such as canals, filled. Mobile telephone numbers were identified that were associated with the fly-tippers enterprise. Subscriber data and service use data acquired on these phones identified where the fly-tipper lived and the addresses he used. On 9th August 2010 at Blackfriars Crown Court the defendant was convicted of offences under the Environmental Protection Act 1990 and the Fraud Act 2006 and was sentenced to 4 months imprisonment.

**Case Study 5**
Leicestershire County Council Trading Standards Service – Car Clocking Scam

Two individuals purchased high mileage cars via vehicle auction sales and reduced their odometer readings using bespoke mileage correction equipment. Cars were subsequently sold to unsuspecting private buyers together with altered MOT certificates and falsified service histories. This form of acquisitive crime allows the fraudster to make substantial financial gains whilst the purchaser is left with a vehicle of minimal resale value. This activity also harms the collective interest of businesses that operate within the retail car trade. An array of names, addresses and telephone numbers were provided by the defendants in advertisements, auction records and sales invoices. Subscriber checks acquired in relation to the telephone numbers enabled investigators to link both defendants to the purchase and sale of around forty vehicles. At Leicester Crown Court, one of the defendants pleaded guilty to conspiracy in undertaking a business for a fraudulent purpose, supplying goods with a false trade description and engaging in unfair commercial practice. He was sentenced to 12 months imprisonment. Following a six day trial his co-defendant was also convicted of conspiracy and received an 18 month prison sentence. A number of the victims who purchased clocked vehicles received compensation, ordered by the Judge to be realised from the confiscation of the defendants' assets.

### Other public authorities

7.47 There are a number of other public authorities that are registered for the purpose of acquiring communications data. These include the Serious Fraud Office (SFO), the Independent Police Complaints Commission (IPCC), the Gangmasters Licensing Authority and the Office of Fair Trading (OFT), to name just a few. The full list of public authorities registered can be found in the Regulation of Investigatory Powers (Communications Data) Order 2010 (No. 480). These public authorities are restricted both in relation to the statutory purposes for which they can acquire data and the types of communications data they can acquire. Only a few of these public authorities are permitted to acquire traffic data under Section 21(4)(a), with the majority only authorised to acquire subscriber and service use data under Sections 21(4)(c) and (b) respectively.

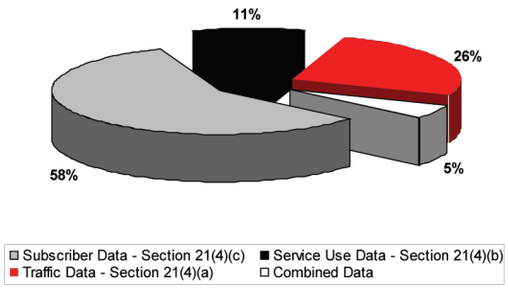
7.48 By comparison with police forces and law enforcement agencies, these 'other' public authorities make very limited use of their powers to acquire communications data. During the period covered by this report 23 of these public authorities notified me that they had made use of their powers to acquire communications data and between them they made a total of 2875 requests. This is an increase from the previous year's figure (1705 requests). However to put this figure in context, it represents just 0.5% of all communications data requests submitted by public authorities. During the course of the reporting year inspections were carried out at 11 of these public authorities. Table 1 lists the public authorities who reported using their powers in 2010 and those inspected are highlighted in red.

Table 1 – All Other Public Authorities who reported using their powers in 2010 (those inspected highlighted in red)

- Common Services Agency for the Scottish Health Service – Scotland Counter Fraud Services
- Criminal Cases Review Commission
- Department for Business, Innovation & Skills (BIS)
- Department for Transport – Rail Accident Investigation Branch
- Department of Health – Medicines and Healthcare Products Regulatory Agency (MHRA)
- Gambling Commission
- Gangmasters Licensing Authority (GLA)
- Independent Police Complaints Commission (IPCC)
- Office of Fair Trading (OFT)
- Police Ombudsman for Northern Ireland (PONI)
- Serious Fraud Office (SFO)
- Cambridgeshire Fire & Rescue Services
- Department for Transport – Maritime & Coastguard Agency
- Department of Food and Rural Affairs (DEFRA) – Investigation Services
- Environment Agency
- Financial Services Authority (FSA)
- Health & Safety Executive (HSE)
- Information Commissioner's Office (ICO)
- Ministry of Justice – National Offender Management Service (NOMS)
- National Health Service (NHS) Business Services Authority – Counter Fraud and Security Management Services Division (CFSMS)
- Northern Ireland Trading Standards Service (NITSS)
- Office of Communications (Ofcom)
- Royal Mail

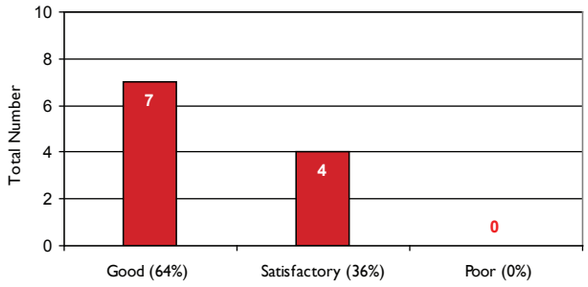
7.49 Once again the largest user by far was the Financial Services Authority (FSA) who made 1885 of the 2875 requests (approx 66%). 52% of the 23 public authorities who reported using their powers made less than 20 requests in the reporting period. Chart 8 illustrates that 58% of the 2875 requests were for subscriber data under Section 21(4)(c). 16 of the 23 public authorities acquired service use data under Section 21(4)(b) and these accounted for 11% of the requests. Only 9 of the public authorities acquired traffic data under Section 21(4)(a) and these accounted for 26% of the requests. The remaining 5% of requests were for a combination of the data.

Chart 8: Other Public Authorities – Percentage of Communications Data Requests by Type




7.50 Chart 9 illustrates that all of the public authorities inspected achieved either a good or satisfactory level of compliance with the Act and Code of Practice. My Inspectors were generally satisfied that communications data was being acquired lawfully and for a correct statutory purpose. The applications were completed to a good standard and my Inspectors were satisfied that the DPs were discharging their statutory duties responsibly.

Chart 9: Other Public Authority Inspection Results 2010




7.51 The comments I have made in the preceding section of the report in relation to submitting telephone numbers for the same investigation on one application to reduce bureaucracy and in relation to ensuring that Section 22(4) Notices are formally issued by the DPs were equally pertinent to some of these inspections. Although the Maritime and Coastguard Agency emerged satisfactorily from their inspection, the Inspector concluded that there was room to improve the quality of their applications and the record keeping in relation to the urgent oral process (which is used in connection with life at immediate risk situations). A series of recommendations were made to assist the Maritime and Coastguard Agency in this respect and I have received an assurance that they have been achieved.

7.52 As previously stated, the largest user was the Financial Services Authority (FSA), which submitted 66% of the requests. The FSA has a statutory objective to reduce financial crime and investigates and prosecutes a range of offences relating to financial services and markets, including insider dealing. The offences are costly to consumers and potentially damage the integrity of UK financial markets. Communications data can be critical in proving whether or not offences have occurred. I would like to highlight one investigation undertaken by the FSA where communications data was used effectively as this may provide a better understanding of its importance to the criminal investigations that the FSA undertake.

**Case Study 6**
Financial Services Authority (FSA) – Operation Duke

The FSA used communications data to successfully investigate and prosecute insider dealers and to locate a missing trader. Suspicions were raised about timely trading by one suspect ahead of announcements which moved the price of shares. Communications data showed that shortly after the insider learned confidential price-sensitive information there was contact between him and his wife, and then between his wife and the trader. When searches were conducted the main trader was missing, but was traced using communications data to an island in the Indian Ocean, from where he was extradited. The trader, the insider and his wife all pleaded guilty to 8 counts of insider dealing, with the proceeds of trading in excess of £2 million pounds. All three received custodial sentences.

7.53 The Inspections confirmed that the aforementioned public authorities restricted the use of their powers to acquire communications data in investigations where they have a clear statutory duty and responsibility to conduct a criminal investigation. A number of these public authorities have other functions or civil enforcement work which does not concern the investigation of criminal offences and it was good to see that they were ensuring that their powers under Chapter II of Part I of RIPA were not used for those purposes.

## Training

7.54 The National Policing Improvement Agency (NPIA) continues to take responsibility for the training and accreditation of police force and law enforcement agency 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 also have the opportunity to keep abreast of the developments in the communications data community and develop their skill level to the best possible standard. NPIA have now extended their communications data training to applicants, intelligence officers, investigators, analysts, DPs and SROs. This will ensure that police forces and law enforcement agencies are able to make the best use of communications data as a powerful investigative tool and will also assist to raise the standards being achieved across the board. There is still a gap in relation to the training that is available to local authorities and other public authorities who are not able to obtain traffic data and it is important for this gap to be filled to ensure that these public authorities are able to maintain their skill level and stay abreast of developments in the communications data community.

## Summary

7.55 My annual report should provide the necessary assurance 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 (FOIA) 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.

7.56 In the reporting year 97 public authorities were inspected by my inspection team. All of the public authorities responded positively to their inspections and there is clear evidence from the inspections that they are committed to achieving the best possible level of compliance with the Act and Code of Practice. I have provided more detailed information in this years report and I hope this provides readers with more insight into the rigour of the inspection process and the effective use being made of communications data.

# 8: INTERCEPTION OF PRISONERS COMMUNICATIONS

## General Background

8.1 I have continued to provide oversight of the interception of communications in prisons in England, Wales and Northern Ireland. This function does not fall within my statutory jurisdiction under RIPA, but the non-statutory oversight regime came into effect in 2002. The intention was to bring prisons within a regulated environment. Section 4(4) of RIPA provides for the lawful interception of communications in prisons to be carried out under rules made under Section 47 of the Prison Act 1952.

8.2 The interception of prisoners' communications plays a vital role not only in the prevention and detection of crime but also in maintaining security, good order and discipline in prisons and in safeguarding the public.

8.3 My inspection team undertake a revolving programme of inspection visits to prisons. The Inspections generally take 1 day and the frequency of each prison's inspection depends on the nature and category of the establishment and their previous level of compliance. The Inspectorate has an excellent working relationship with the National Intelligence Unit (NIU) at the National Offender Management Service (NOMS) and regular meetings are held to review the outcomes of the inspections.

## Inspection Regime

8.4 The primary objective of the inspections is to ensure that all interception is carried out lawfully in accordance with the Human Rights Act (HRA), Prison Rules, Function 4 of the National Security Framework (NSF) and the Public Protection Manual (PPM). Interception is mandatory in some cases, for example in relation to 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.

8.5 A legal obligation is placed upon the Prison Service to inform the prisoners, both verbally and in writing that their communications are subject to interception. Good evidence must be created and retained to demonstrate this legal obligation is being fulfilled. My Inspectors examine the arrangements in place to inform prisoners that their communications may be subject to interception. All prisoners must sign the national Communications Compact issued by the Chief Executive, NOMS in November 2008. My Inspectors randomly examine signed copies of the Communications Compacts to check that they are being appropriately issued. They also check that notices regarding the interception of communications are displayed within the prison.

8.6 The systems and processes in place for identifying and monitoring prisoners who are subject to offence related monitoring, intelligence-led monitoring or monitoring for other security / control issues (i.e. Category A prisoners, Escape List prisoners, ad hoc and random monitoring) are examined. The Interception Risk Assessment process and the authorisations in place for the monitoring (if required) are scrutinised. My Inspectors check that there are proper procedures in place for reviewing the continuation of the monitoring of these prisoners communications.

8.7 The system in place for the recording and monitoring of telephone calls will be examined, along with the monitoring logs that are maintained by the staff conducting the monitoring. Similarly the systems and procedures in place for the monitoring of prisoners correspondence (mail), along with the monitoring logs that are maintained by the staff conducting this monitoring, are examined. There must be a full audit trail in place in relation to all communications that are intercepted.

8.8 The Inspectors examine the procedures in place for the handling of legally privileged or confidential communications. The provisions for the retention, destruction and storage of intercept material are examined.

8.9 The Inspectors also examine the processes relating to the disclosure of material to law enforcement agencies to ensure they are fully aligned to the Police Advisers Section (PAS) Operational Guidance Documents (OGD3 & 4).

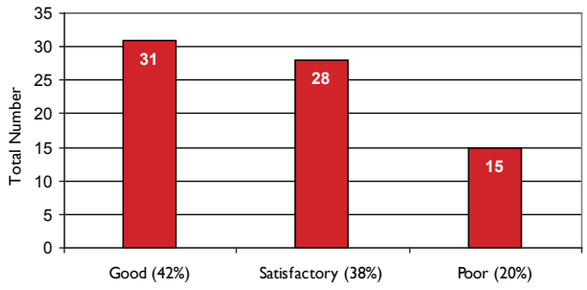
8.10 Following each inspection a detailed report is prepared and this outlines inter alia what level of compliance has been achieved with the rules governing the interception of prisoners' communications. I have sight of all of the inspection reports in order to discharge properly my oversight functions. Where necessary, an action plan will accompany the report which specifies the areas that require remedial action. A copy of the report is sent to the Governor or Director of the prison. They are required to confirm, within a prescribed time period, that the recommendations have been achieved or outline the progress they have made against achieving the recommendations. All of the reports are also copied to NIU and the Deputy Director of Custody for the relevant prison region.

**Review of 2010 Prison Inspections**

8.11 There are 132 prisons in England & Wales subject to inspections and 3 in Northern Ireland. Since the Inspectorate was formed virtually all of them have been inspected at least three times. During the period covered by this report my Inspectors conducted 77 inspections at 74 prisons, which equates to over 50% of the whole estate.

8.12 Chart 10 illustrates that 80% of the prisons achieved either a good or satisfactory level of compliance overall.

Chart 10: Prison Inspection Results 2010




8.13 The vast majority of prisons had either partially or fully implemented their previous recommendations and as a result the majority had improved their level of compliance with the rules governing the interception of prisoners' communications. My Inspectors found examples of good practice firmly embedded in the systems and processes in some of these prisons. In a number of the establishments the managers and staff clearly demonstrated a commitment to achieve the best possible standards.

8.14 Regrettably serious weaknesses and failings were found in the systems and processes of 15 of the prison establishments which were inspected. Considering the fact that it was either the third, fourth or in one instance the fifth inspection of these establishments, my Inspectors would have expected to see much better standards being achieved. These prisons had mostly either ignored or failed to fully implement the recommendations from their previous inspections. This number has reduced from the previous year, but it is still too high and indicates a failure by managers and staff to ensure the interception of communications is conducted fully in accordance with the rules. Three of these prisons were visited twice during the reporting year. I am pleased to report that the re-inspection of one of these prisons found a complete transformation and consequently that establishment is now achieving a good level of compliance. Regrettably my Inspectors concluded that the other two establishments had not made significant progress during the re-inspections and were still achieving a poor level of compliance. This is concerning considering the fact that they were subject to two inspections in the reporting year. These prisons have now provided an assurance that they will take the necessary remedial action, nevertheless they will again be subject to an early re-inspection to check that they have improved.

8.15 Last year I reported that serious weaknesses and failings were found in relation to the issuing and filing of the Communications Compact in 52 prisons which was a cause for concern. This year my Inspectors found failings to follow the correct procedures in this aspect of the process in 31 prisons. In 3 establishments the Communications Compact was not in evidence at all. 6 establishments had failed to introduce the current version of the Compact and 6 of the establishments were not carrying out checks on the prisoners legal contact numbers. Following these inspections recommendations were made to remedy the failings and I have been assured that they

have been implemented. On the whole this was an improvement on the findings from the previous year even though it was the first time that a number of these prisons had been inspected since the Compact measures were introduced. The vast majority of prisons have now been subject to an inspection since this time and therefore next year I hope to report that a larger number of prisons are compliant in this aspect of the process.

8.16 Failure to monitor the communications of prisoners who pose a risk to children, the public or the good order, security and discipline of the prison could place managers and staff in an indefensible position if a serious incident was to occur which could have been prevented through the gathering of intercept intelligence. In a number of the establishments inspected the monitoring of prisoners who pose a risk to children or the public is still a weak area. Having said that I do not necessarily imply that prison managers and their staff are deliberately setting out to circumvent the rules because 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. 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 more effectively. In 19 of the establishments inspected this year the failures were directly related to the fact that the targets being set were completely unrealistic and unattainable and a huge increase in staff and equipment would have been 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 necessarily 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.

8.17 Last year I reported that the new version of the NSF stipulated that Interception Risk Assessments should be in place before an authorisation is granted to monitor a prisoner's communications. Interception Risk Assessments create good evidence to show that the risk factors have been taken into account and support the Authorising Officers decision as to whether monitoring is necessary or not. I am pleased to report that 45 of the prisons inspected had introduced Interception Risk Assessments into their process and these have had a marked effect in reducing the number of prisoners requiring monitoring. This has enabled the monitoring staff in these prisons to focus their efforts upon the prisoners who pose the highest risk and has made the monitoring more effective. 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 and a number of the prisons have already adopted this strategy. This has enabled these prisons to free up resources to conduct more intelligence-led monitoring in relation to prisoners who pose a threat to the security or good order and discipline in the prison as they are, for example, smuggling drugs or illicit mobile telephones into the establishment.

8.18 The authorisations in place to conduct the offence related and intelligence-led monitoring were examined by my Inspectors and regrettably a number of establishments had failed to take on board the reduced authorisation periods which came into force when the revised NSF was published in February 2009. Offence related monitoring must now be reviewed at least every 3 months and reviews for intelligence-led monitoring must now be undertaken within 1 month. 17 of the establishments were still approving offence related monitoring for a period of 6 months and 12 of the establishments were still approving intelligence-led monitoring for a period of 3 months. Recommendations have been made for these establishments to align their authorisations to the NSF and to ensure that they introduce a robust review process so that monitoring does not continue if an authorisation has expired.

**Summary**

8.19 In the reporting year 77 prison inspections were conducted by my inspection team. All of the prisons responded positively to their inspections and overall the responses to the recommendations have been encouraging. The prisons which have a dedicated team of well trained staff to conduct the interception of communications always achieve much better standards and it is pleasing that a number of establishments are moving towards introducing this good practice system.

8.20 In previous inspection reports I have 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 prisoners' communications. The start date of the pilot was delayed, but I am pleased to report that it eventually started in October 2010. The pilot is still ongoing and I will therefore not be able to report on the findings until next year's annual report.

8.21 My resources only enable approximately half of the establishments to be subject to an inspection each year and therefore the findings from the prison inspections are likely to go in two year cycles. This year it has been clear that managers and staff are becoming more accustomed to the process and have a better understanding of the systems and procedures that should be in place. There is evidence from a number of the inspections that managers and staff are committed to achieving the best possible level of compliance with the rules governing the interception of prisoners' communications.

# 9. INVESTIGATORY POWERS TRIBUNAL

9.1 The Investigatory Powers Tribunal (the IPT) was established by section 65 of RIPA and came into being on 2 October 2000. From that date the IPT assumed responsibility for the jurisdiction previously held by the Interception of Communications Tribunal, the Security Service Tribunal and the Intelligence Services Tribunal, in addition to the complaints function of the Commissioner appointed under the Police Act 1997 as well as for claims under the Human Rights Act. The current President of the Tribunal is Lord Justice Mummery with Sir Michael Burton acting as Vice-President. In addition, eight senior members of the legal profession served on the Tribunal in 2010, one of whom stepped down in April 2010.

9.2 As I have explained in my previous Annual Reports, 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 164 new applications during the calendar year 2010 and completed its investigation of 208 cases during the year. 40 cases have been carried forward to 2011.

### Assistance to the Tribunal

9.3 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 2010.

### Determinations made by the Tribunal in favour of complainants

9.4 During 2010 the Investigatory Powers Tribunal made six determinations in favour of complainants. Since its inception the Investigatory Powers Tribunal has now upheld ten complaints. One of the upheld complaints was made by a husband and wife who lodged a joint complaint and five by members of the same family. On the grounds of confidentiality, the Investigatory Powers Tribunal Rules 2000 prohibit me from disclosing specific details about the complaint made by the husband and wife, but it is sufficient to say that the conduct complained of was not authorised in accordance with the relevant provisions of RIPA. The complaints made by the five members of the same family were the subject of an open hearing in November 2009 which was widely reported in the media. The case involved directed surveillance carried out by Poole Borough Council of a family in connection with an application made by the parents for a school place for their youngest child. The Tribunal found that the conduct complained of was not authorised in accordance with the relevant provisions of RIPA. The complainants made no application for remedies and none were awarded. The fact that these cases were upheld has led to changes in guidelines provided to Local Authorities on the use of directed surveillance and proposed legislation to change the procedures on the authorisation of this type of surveillance.

# 10. CONCLUSION

10.1 The interception of communications continues to play a vital role in the battle against serious crime and terrorism currently being fought by the UK's law enforcement and security agencies. It remains, however, a powerful method and one which has the potential to intrude significantly into the private life of an individual. For this reason, there are I believe a number of key principles that work well in this country and should continue to form the building blocks of any successful interception system in the future.

10.2 First, the role of a Secretary of State or Scottish Minister as an elected individual signing off acts which may involve intrusion into the private life of a citizen is, in my view, crucial. This year, as in previous years, I can report with confidence that the Secretaries of State I have met during the course of the year take significant care to ensure that each warrantry authorisation they sign is necessary and proportionate as required by RIPA, but in addition to this is based on an in-depth assessment of legal, operational and wider risks. The agencies are aware, as I mentioned earlier, that the Secretary of State or Scottish Ministers are not simply 'rubber-stamping' requests presented to them

10.3 Secondly, it is my belief that Secretaries of State or Scottish Ministers could not undertake their role without the level of in-depth submissions provided to them by officials within intercepting agencies. The greatest assurance the public may derive is that an authorisation request crosses the desks of a number of officials and, if necessary, legal advisers and is scrutinised with some considerable care before it reaches the Secretary of State or the Scottish Ministers. It is my view that during an era of increasing threat and greater sophistication of terrorists, criminals and hostile states, Ministers and intelligence and law enforcement agencies undertake the work which I am required to oversee with diligence and in accordance with the law.

10.4 Thirdly, I feel it is important during a period of potential reform to intelligence oversight to highlight the strengths of my independent oversight function and constructive relationship with the agencies. This relationship is based on trust, mutual understanding and constructive comment. As mentioned earlier, I have never had to demand access to files and indeed have been provided with more operational detail behind warrants than is strictly necessary, enabling me to provide a better assessment of the necessity and proportionality behind applications for interception.

10.5 I believe the agencies welcome my oversight and on occasions they consult me before particularly complex operations and investigations. That is not to say, however, that the agencies are not willing to make changes based on my own and wider oversight of their activities. Readers will be aware that in this year's annual report I have detailed, where possible without prejudicing national security, the nature of my inspection visits, year-on-year changes in numbers of errors reported by agencies and most importantly details of better working practices that have been implemented after errors have occurred. The statistics presented show that there has been a reduction of close to 50% in the number of interception errors reported by those agencies over the last three years during a time of increased overall threat from serious crime and terrorism. This is in no small part due to a productive working relationship between the agencies and myself in addition to increasingly better understanding within the agencies of the

legal, human rights and wider ethical bases of interception. I have provided more detailed information in this years report and I hope this provides readers with more insight into the rigour of the inspection process and the effective use being made of interception and communications data.

10.6 I would also like to restate, as in previous years, that my work would not be possible without the support provided by the small secretariat working with me. I would also extend my thanks to both Sir Mark Waller and Sir Peter Gibson, current and former Intelligence Services Commissioners, and members of the Investigatory Powers Tribunal. They, and the team of Inspectors I have referred to previously, have all done excellent work, and for this I continue to be very grateful.

10.7 Lord Bingham of Cornhill, who died recently, was one of my predecessors as Commissioner in 1992-1993, and I take this opportunity to acknowledge his contribution in this, as in so many other, spheres.

# Annex A: Public authorities listed under RIPA in the UK

## 1a POWERS TO INTERCEPT COMMUNICATIONS

### LAW ENFORCEMENT AND INTELLIGENCE

- Intelligence Services
  - Security Service(SyS)
  - Secret Intelligence Service (SIS),
  - Government Communications Headquarters (GCHQ))
- Serious Organised Crime Agency (SOCA)
- Scottish Crime and Drugs Enforcement Agency (SCDEA)
- Metropolitan Police (Met)
- Police Service for Northern Ireland (PSNI)
- Scottish Police forces
- HM Revenue and Customs (HMRC)
- Defence Intelligence Staff (DIS)

## 1b POWERS TO ACQUIRE COMMUNICATIONS DATA

### LAW ENFORCEMENT AND INTELLIGENCE

- Intelligence Services (SS, SIS, GCHQ)
- Police Forces (HO, Met, City, Scotland, PSNI)
- Military Police Forces (Army, Navy, Air Force)
- Ministry of Defence Police
- British Transport Police
- Ports Police (Merseyside, Dover)
- Civil Nuclear Constabulary (CNC)
- Serious Organised Crime Agency (SOCA)
- Scottish Crime and Drug Enforcement Agency (SCDEA)
- HM Revenue and Customs (HMRC)
- Independent Police Complaints Commission(IPCC) /
- Office of Police Ombudsman for NI

### IMMIGRATION, ASYLUM, PRISONS AND DETENTION CENTRES

- Home Office UK Border Agency (UKBA)
- Ministry of Justice – National Offender Management Service (NOMS)
- NI Office (Prison Service) (in 2010 consolidating order)

**OTHER GOVERNMENT DEPARTMENTS**

- Department of Agriculture and Rural Development for NI
- Department of Business, Innovation and Skills
- Department of Enterprise, Trade and Investment for NI
- Department for Environment, Food and Rural Affairs
- Department of the Environment in NI (2010 consolidating order)
- Department of Health (Medicines and Healthcare Products Regulatory Agency)
- Department for Transport – Air / Marine / Rail Accident Investigation Branches
- Department for Transport – Maritime & Coastguard Agency
- Serious Fraud Office

**EMERGENCY SERVICES**

- Ambulance Services (England, Wales, Scotland, NI)
- Fire Services (England, Wales, Scotland, NI)
- Police Forces (HO, Met, City, Scotland, PSNI)

**REGULATORY BODIES**

- Charity Commission
- Child Maintenance and Enforcement Commission (2010 consolidating order)
- Financial Services Authority
- Food Standards Agency
- Environment Agency / Scottish Environment Protection Agency
- Gangmasters' Licensing Authority
- Gambling Commission
- Health and Safety Executive (HSE)
- Information Commissioner
- Office of Communications (OFCOM)
- Office of Fair Trading
- Pensions Regulator
- Postal Services Commission

**OTHER BODIES**

- Criminal Cases Review Commission (CCRC)/ Scottish CCRC
- Local Authorities (England, Wales, Scotland and NI)
- NHS bodies (National Health Service Business Services Authority / NI Health & Social Services Central Services Agency / Common Services Agency for the Scottish Health Service)
- Royal Mail

Only certain sections and individuals within the above organisations can obtain authorisations for the acquisition and disclosure of communications data. These are listed in full in RIPA Statutory Instrument 2010 No.480, which is available at the following link http://www.legislation.gov.uk/uksi/2010/480/schedule/1/made

TSO
information & publishing solutions

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

**Online**
**www.tsoshop.co.uk**

**Mail, telephone, fax and email**
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
Email: 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
Telephone orders/general enquiries: 028 9023 8451
Fax orders: 028 9023 5401

HO_01054_G

ISBN 978-0-10-297407-2

9 780102 974072