2011 Annual Report of the Interception of Communications Commissioner

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 on 13th July 2012

Laid before the Scottish Parliament by the Scottish Ministers July 2012

HC496
SG/2012/125

£16.00

2011 Annual Report of the Interception of Communications Commissioner

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 on 13th July 2012

Laid before the Scottish Parliament
by the Scottish Ministers
July 2012

HC496
SG/2012/125

London: The Stationery Office £16.00

Any enquiries regarding this publication should be sent to us at c/o Interception of Communications Commissioner, 2 Marsham Street, London SW1P 4DF

This publication is available for download at www.official-documents.gov.uk.
This document is also available from our website at www.intelligencecommissioners.com

ISBN: 978-0-10-298032-5

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

ID 22445689 07/12

Printed on paper containing 75% recycled fibre content minimum

BIOGRAPHY AND INTRODUCTION

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 was appointed President of the Court of Appeal in Gibraltar in 2011, having been a member since 2006.

Sir Paul will serve as Commissioner until 31st December 2012.

1. CONTENTS

2. COMMISSIONER'S FOREWORD

I am required by Section 58 (4) of the Regulation of Investigatory Powers Act (RIPA, 2000) to report to the Prime Minister 'as soon as practicable after the end of each calendar year' with respect to the carrying out of my functions. Having undertaken this act annually since 2006, I move now to my penultimate report, covering the period between 1st January to 31st December 2011.

Much has changed in interception and the use of communications data since I began as commissioner in 2006. Changes have been caused by the advancement of communications technology, and the increase in methods of communication available to members of the public. Lawful interception and/or communications data acquisition remain crucial techniques for the UK's intelligence agencies, law enforcement bodies and selected other public authorities to use in pursuit of their statutory objectives. I remain confident that they and the warrant-signing Secretaries of State whom I oversee, take very seriously their responsibilities to comply with the legislation.

In last year's annual report, I responded to valuable feedback from amongst others the media and members of the public. I was able to provide more detail than ever before on:

- the legislative basis underpinning the lawful interception of communications by those public authorities with powers under RIPA.
- the warrantry authorisation process, including the role of the senior official, the department of state and ultimately the Secretary of State
- case studies describing where lawful interception and communications data had played a central role in achieving operational successes
- year-on-year changes in warrant numbers signed by the Home Secretary and Scottish Ministers
- year-on-year changes in communications data requests submitted by public authorities
- year-on-year changes in numbers of errors reported to me by public authorities in relation to both lawful intercept and communications data; and
- as far as I was able to disclose them, the nature of the errors reported to me, and the actions taken to minimise the risk of such errors being repeated in the future.

The report for 2010 was on the whole well received, and I report in similar depth this year. I have repeated information which I believe is necessary in order that readers may understand the use of lawful interception, communications data and my oversight without reference to previous reports. I disclose the following additional information this year, which may assist readers to understand my ultimate conclusion that public authorities are achieving a very good standard of compliance subject to the issues described in this report.

- more detail on when and how my inspectors and I have conducted our scrutiny visits, whom we have met and broad details of the kinds of cases and issues on which my formal and informal input, and that of my inspectors, has been requested.
- more detail on the distinctions between the authorisation processes and oversight mechanisms in relation to lawful interception (Part I, Chapter I, of RIPA) and the acquisition of communications data (Part I, Chapter II of RIPA)

- the number of RIPA lawful interception warrants signed by Secretaries of State and Scottish Ministers
- the causes of the communications data errors in 2011
- the number of recommendations emanating from the communications data inspections in 2011
- details of my meetings with counterparts engaged in intelligence oversight globally and in the UK
- my responses to consultations (so far as they can be disclosed) and speeches I have delivered on my role as commissioner
- examples of how the Intelligence Services Commissioner, Sir Mark Waller and I have responded to demands for greater transparency. Much of this information can be found by readers on the commissioners' website www.intelligencecommissioners.com, which was launched in 2011

As indicated above I disclose this year for the first time in this part of my report the total number of lawful interception warrants signed by Secretaries of State and Scottish Ministers. No more detail is required to evaluate the work of the overseer, and any further breakdown of numbers in an open report could be of assistance to criminals or those who pose a threat to national security.

In a similar way I can seek to explain the oversight procedure which I use, but, for obvious reasons, I cannot refer to specific warrants or authorisations, or to confidential discussions I have had with those whom I oversee.

Some matters which cannot be included in an open report may nonetheless be disclosed to Ministers and certain senior intelligence officials so that, at a time when changes are being considered, they can have a better understanding of what is being overseen, how it is being overseen, and the impact of such oversight. In order to facilitate this I have produced a confidential annex which I am hopeful will be made available to that limited audience.

3. LEGISLATIVE BASIS - AN INTRODUCTION TO PART I OF RIPA

Previous commissioners have outlined in their respective annual reports the scope of each part of RIPA, the functions of the intelligence services and the functions of the commissioner. In addition, in my 2010 annual report, I sought to aid understanding of RIPA by presenting its key components in relation to lawful intercept and communications data in a summary diagram. This was well received and the summary grid can be found on the commissioners' website (www.intelligencecommissioners.com)

RIPA and the way in which it tightly defines both the remit of the commissioner, the lawful interception of communications and the acquisition of communications data is still often misunderstood by both the media and wider public, so once again, I draw attention to the following

- a summary grid (Table 1) outlining the relevant sections of the statute governing the use of RIPA powers.
- my remit, as set out in section 57 (2) of RIPA, being the terms and conditions upon which I accepted the role of commissioner.

Table 1 – RIPA Summary Box

Which section of RIPA?	What is the Power?	When can this power be used?	Who can use the power?	Who authorises use of this power?	Who oversees the responsible use of power?
Pt. I Chapter I	Interception of a persons communications (i.e. telephones, emails, texts, post).	In the interests of national security. Prevention and detection of serious crime. Safeguarding the economic well-being of the UK.	Intelligence Services: – Government Communications Headquarters (GCHQ) – Security Service (SyS) – Secret Intelligence Service (SIS) 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).	Any of the Secretaries of State, but in practice the Secretary with responsibility for the investigating body will sign their respective warrants.	Oversight conducted by the Interceptions of Communications Commissioner.

Which section of RIPA?	What is the Power?	When can this power be used?	Who can use the power?	Who authorises use of this power?	Who oversees the responsible use of power?
Pt. I Chapter II	The acquisition of communications data (the 'who', 'when' and 'where' of a communication). The distinction between this and the interception of a communication will be further clarified in the following parts of this report.	In the interests of national security. Prevention and detection of crime or prevention of disorder. Safeguarding the economic well-being of the UK. In the interests of public safety. For the purpose of protecting public health. For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department. For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. For any additional purpose specified by an order from the Secretary of State.	A wider group of public authorities can use the powers provided under Chapter 2 of the act than those under Chapter 1, including police forces, intelligence agencies, other enforcement agencies and local authorities. The full list of public authorities and their respective authorising personnel can be found in the Statutory Instrument (SI) at http://www.legislation.gov.uk/uksi/2010/480/pdfs/uksi_20100480_en.pdf. It is important to note that although the list of bodies is larger, they have not all been given the same powers. The bodies are restricted in both the statutory purposes for which they may acquire data under Section 22(2) and the type of data they may acquire under Section 21(4). These restrictions will be discussed later in my report..	A senior official in that public authority (as specified on the SI link).	Oversight conducted by the Interceptions of Communications Commissioner through a team of inspectors.
Pt. III	The investigation of electronic data protected by encryption.	Interests of national security. Prevention / detection of crime. Interests of economic well-being of United Kingdom; or 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.	Oversight is conducted by the Interception of Communications, Intelligence Services and Surveillance Commissioners, except when authorised by a judge.

3.1. Part I, Chapters I and II of RIPA – Lawful Intercept and Communications Data

It may be helpful to restate here the difference between lawful interception and acquisition of communications data. Both fall under the remit to oversee, but they are differently authorised and used to different extents.

The power to acquire the content of a communication, be it an email, telephone call or SMS message, is provided under Part I, Chapter I of RIPA. It requires a warrant signed by a Secretary of State or Scottish Ministers.

Part I, Chapter II of RIPA, provides the power to acquire communications data. This represents the 'who', 'when' and 'where' of a communications event, and requires an authorisation by a designated person of an appropriate grade within the public authority with the requisite powers under RIPA.

I set out in the section that follows details of the legislative provisions within RIPA in relation to lawful interception and the acquisition of communications data. In addition, (in order to aid understanding of the distinction between communications data and lawful interception) I have set out the different authorisation processes and inspection regimes employed by myself and my inspectors to check compliance in relation to lawful intercept and the acquisition of communications data.

4. MY AREAS OF OVERSIGHT

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 powers and duties conferred or imposed on him by or under sections 1 to 11." This refers to the use of, and authorisation systems in place to control the use of, lawful intercept techniques. What is meant by lawful intercept techniques is more fully explained in section 6.
- "The exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I." Put simply, this is my assessment, through a team of inspectors, of the performance of the public authorities that can acquire communications data. We check that the public authorities are using the 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." This refers to the investigation of electronic data protected by encryption etc.
- "The adequacy of the arrangements by virtue of which (i) the duty which is imposed on the Secretary of State by section 15, and (ii) so far as applicable to information obtained under Part I, the duties imposed by section 55, are sought to be discharged." This refers to the safeguards put in place for the protection of the material gathered.

In essence my inspectors and I act as auditors. We look at the materials on which decisions were made, how those materials were 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.

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 2011, but when sought it has willingly been given.

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.

In addition my predecessor agreed to undertake the oversight of the lawful interception of the communications of prisoners, and my inspectors have continued to do that work.

My remit is therefore quite extensive, but it is circumscribed. I do not have blanket oversight of the intelligence or law enforcement agencies, and I am not authorised to oversee all of their activities. But I do have a constructive relationship with them. They consult me, and I assist when I can.

5. SUCCESSES

I continue to be impressed, as in previous years, with the role that lawful interception and communications data acquisition play in the operational successes of law enforcement agencies in the UK. Interception remains a powerful technique in the investigation of many kinds of crime and threats to national security. Many of the largest drug-trafficking, fiscal evasion, people-trafficking, counter-terrorism and wider national security and serious crime investigative successes of the recent past have in some way involved the use of interception and communications data.

The following case summaries are just a sample of a large number of operations that have featured in the national media or have been identified during inspections where lawful interception or communications data (or both) have played a role in a successful outcome. Thus I hope to highlight the successful use of lawful intercept to combat serious crime as well as the effective use of communications data by the security services, the police and local councils. I have, as in previous years, in order not to prejudice national security, provided detailed examples of other operations in the confidential supplementary reports.

Lawful interception and communications data techniques cannot be used in isolation; they are 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 lawful interception and communications data, they have the potential to be highly intrusive tools. 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.

I have provided further case studies illustrating operational successes in other parts of this report.

Case Study 1 – SOCA use of Lawful Intercept Product

Background: This report concerns a SOCA investigation undertaken between 2009 and 2012. The details have been sanitised. Originating from a SOCA operation into the money laundering activities of a UK-based organised crime group (OCG), two senior members of the OCG were identified as controlling its activities. The operational team had encountered significant difficulties in using conventional investigation techniques. As a result, SOCA considered it necessary and proportionate for these OCG members to be subject to interception.

Interception commenced in early 2009, quickly confirming that the OCG was well established, and involved not only in money laundering but also in the importation of significant amounts of Class A drugs.

Operational Activity: Intercept intelligence made it possible to identify individuals involved in the transportation and storage of drugs on behalf of the OCG. The intelligence enabled SOCA officers to seize the drugs as they were being delivered to OCG members. This resulted in a number of arrests and the seizure of over 100 kilograms of Class A drugs, 1,400 kilograms of Class B drugs and the dismantling of this section of the OCG.

Intelligence later established that a linked OCG was importing Class A drugs using an alternative method. Interception enabled these individuals to be identified and disclosed the location of a consignment of drugs. This intelligence resulted in the seizure of over 150 kilograms of Class A drugs and over £300,000 in cash.

Throughout 2010, interception identified other OCG members who were involved in money laundering on behalf of this OCG. This intelligence enabled the operational team to gather evidence of OCG members conducting this laundering activity, before arresting them and recovering in excess of £600,000.

Intercept product had also shown that the OCG was supplying drugs to local criminals, several of whom were of interest to their respective Police Forces. Intelligence was provided to those Forces as to the activities of these individuals. This resulted in the arrest of over 15 local drugs distributors and the recovery of Class A drugs, money and ammunition. In mid 2010, interception confirmed that a significant Class A drugs supplier, originally linked to this OCG, was in addition distributing drugs to another key OCG in the UK. Subsequent interception of this additional OCG enabled its members to be identified, along with the locations of drugs storage facilities and exchanges. The intelligence derived from intercept led to the seizure of over 100 kilograms of Class A drugs, £200,000 in cash and a firearm.

Interception in 2011 showed that the primary members of the OCG had resumed importations of Class A drugs into the UK and were arranging for customers to collect consignments. Intercept intelligence later identified the locations of drugs exchanges, which resulted in seizures of over 150 kilograms of Class A drugs, 75 kilograms of Class B drugs and several arrests.

Conclusion: This operation lasted just over three years, during which interception played a crucial role in helping law enforcement officers to dismantle at least three linked OCGs involved in importing and distributing Class A drugs within the UK. It has also led to the identification of numerous suppliers based aboard and other persons of interest to law enforcement in the UK. Some of these individuals are now the subject of other SOCA operations.

As a direct result of intelligence provided through interception, in excess of 400 kilograms of Class A drugs, 1,700 kilograms of Class B drugs, three firearms and £1,000,000 in cash have been seized.

In addition, more than 75 people associated with the OCGs outlined have been arrested for drugs supply and distribution, money laundering and firearms possession offences.

Of those subject to interception, approximately one third of individuals have been convicted for drugs-related offences and have received prisons sentences averaging over 15 years each. Intelligence also indicates that the other previously warranted subjects have either fled the UK through fear of prosecution or have curtailed their criminal activities through lack of funds or loss of face within the criminal fraternity.

Intelligence derived from intercept product has increased the understanding of how this and other OCGs operate, including furthering knowledge on importation methods, money laundering processes and the use of technology by criminals.

During the course of this operation, actionable intelligence was disseminated by SOCA to the Association of Chief Police Officers (ACPO) forces and international law enforcement partners. This provided a valuable contribution to law enforcement efforts in the UK and abroad.

Case Study 2 – Dorset Police use of Communications Data

Operation Rally - Dorset Police used communications data to very good effect when investigating a violent robbery of a pensioner that occurred at an isolated dwelling in March 2011. The victim was bound and physically tortured over a two hour period by three masked men. Eventually the victim provided the offenders with access to two safes and as a result 20 firearms, thousands of rounds of ammunition and £4,000 cash were stolen. The case became a force priority with the main objectives being to recover the firearms and minimise the risk to the public.

A range of communications data was acquired in relation to the case; this led to a significant telephone number linked to the offence being identified. Analysis of the communications data associated to that phone led to the identification of mobile phones linked to the offenders. Analysis of the phone data was able to prove communication between the offenders, as well as evidencing their presence in the vicinity at the time of the offence. Further analysis evidenced their collective movement to the scene.

The communications data in this case formed the main strand of the prosecution case and excellent quality analytical charts were prepared for court. Ultimately three defendants were found guilty of robbery and received indeterminate sentences (IPPs) which in effect represent 15+ years' conventional prison sentences. The co-ordinator of the offence was sentenced to 12 years imprisonment. The final defendant received a sentence of 12 months for the possession of firearms

Case Study 3 – Westminster City Council use of Communications Data

Communications data was used effectively in one investigation relating to a dishonest locksmith who tricked vulnerable victims (who had either been burgled or locked out of their houses), by carrying out unnecessary repairs and demanding extortionate sums. The estimates were usually in the region of £98 to £128 in order for him to gain entry into the victim's premises, however once entry had been obtained, via drilling through the lock, he informed the victims that new locks would be required in order to make the premises secure at a further cost of £200 - £300. A number of those he preyed on were elderly or lone women with children. Statements were obtained from 36 witnesses and an expert locksmith examined the suspect's work and concluded that unnecessary work had been carried out and the costs should have been in line with the initial estimates.

Complainants supplied Westminster Trading Standards with the telephone numbers shown in the locksmith's adverts for his companies which operated throughout London and the Home Counties. Subscriber data was acquired in relation to the telephone numbers used by the suspect in connection with his trade and this data enabled investigators to link the companies to the suspect.

At the Central Criminal Court on 22 July 2010 after a 5 week trial, the defendant was found guilty of all 15 sample counts brought against him under the Fraud Act 2006. He was remanded in custody pending probation reports and was sentenced on 31st August 2010, to 4 years imprisonment. He was further banned from acting as a company director for 5 years. A confiscation investigation under the Proceeds of Crime Act 2002 is ongoing with a full confiscation hearing scheduled to take place in April 2012.

6 LAWFUL INTERCEPTION OF COMMUNICATIONS (RIPA PART I, CHAPTER I)

6.1. General Background to Lawful Interception

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).

Interceptions of Communications covered by RIPA are defined in Part I, Chapter I, section 2(2);

> *"For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he —*
>
> *a. so modifies or interferes with the system, or its operation*
>
> *b. so monitors transmissions made by means of the system, or*
>
> *c. so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,*
>
> *as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."*

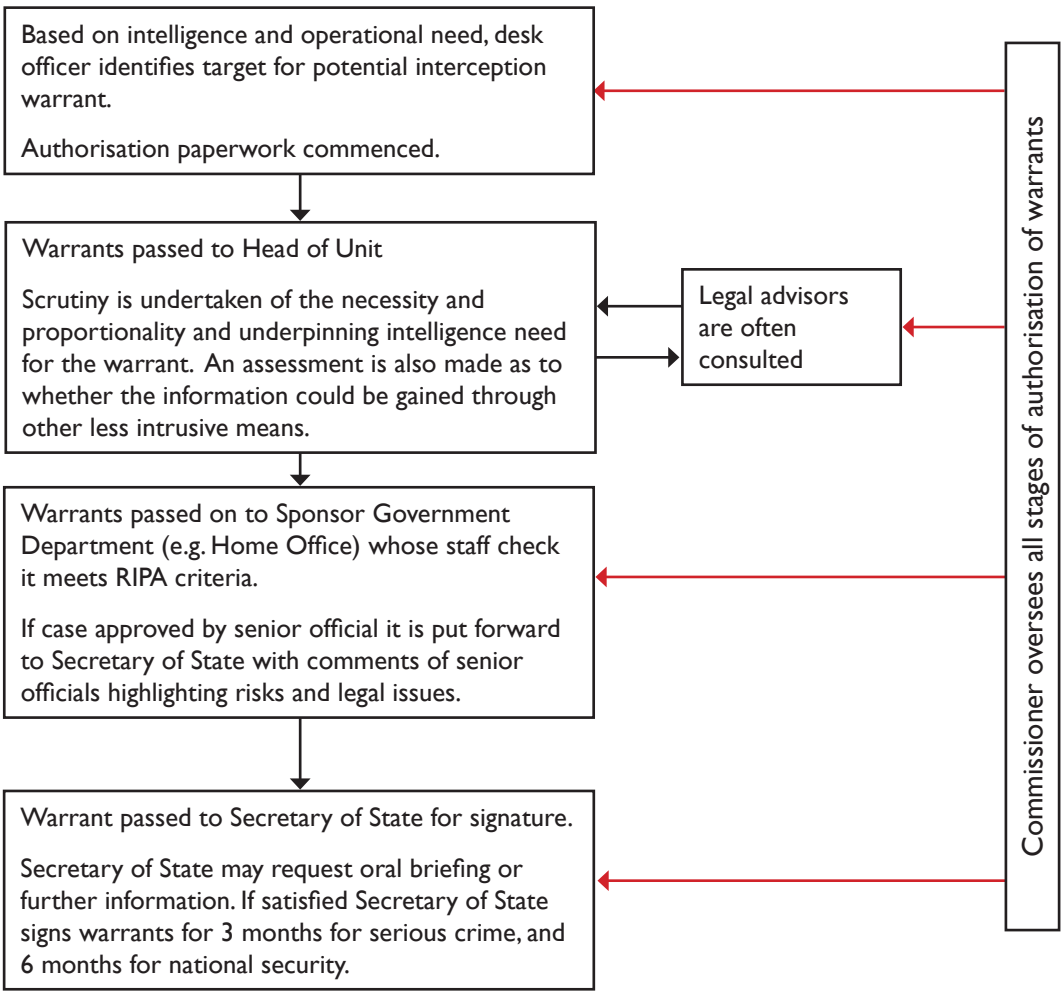
and section 2(4);

> *"For the purposes of this Act the interception of a communication takes place in the United Kingdom if, and only if, the modification, interference or monitoring or, in the case of a postal item, the interception is effected by conduct within the United Kingdom and the communication is either—*
>
> *a. intercepted in the course of its transmission by means of a public postal service or public telecommunication system; or*
>
> *b. intercepted in the course of its transmission by means of a private telecommunication system in a case in which the sender or intended recipient of the communication is in the United Kingdom."*

Due to the potential level of intrusion into an individual's private life associated with lawful 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] to fulfil statutory objectives.

1 Scottish Ministers are the appropriate authority in relation to serious crime in Scotland

Figure 1 - The Warrantry Authorisation Process



As detailed in Figure 1, the role of the Secretaries of State and Scottish Ministers as democratically elected individuals signing off acts which may involve intrusion into the private lives of citizens is very important. 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 lawful interception.

6.2. Inspection Regime

There has been, over the recent past, significant interest in the commissioners' inspection visits in relation to lawful interception under Part I, Chapter I of RIPA. In order to add useful context therefore, this year I present in this section, to the extent allowed without revealing sensitive details, further information on how such inspection visits are conducted.

As outlined in my 2010 Annual Report my primary role in relation to the oversight of lawful interception is that of an auditor retrospectively examining interception warrants twice a year. I visit each agency entitled to obtain authority to intercept. Before each visit I obtain a full list of extant warrants, and lists of warrants which have been modified or cancelled since my last visit. From these lists I make my selection of warrants to be examined in depth at the time of my inspection. Sometimes the agencies draw attention to warrants which they consider that I should review, but it is important that to a substantial extent the selection should be random. I am satisfied that the lists supplied to me are complete. If they were not the omission would be likely to emerge because I also inspect the warrantry documents held by those Departments of State from which warrants can be obtained.

When the inspection takes place I am able to read the paperwork presented to the Secretary of State, and am often assisted by agency staff in relation to the background and the benefit derived from the warrant. I need to be satisfied that at the time when the warrant was obtained the Secretary of State or Scottish Minister was entitled to conclude that it was necessary and proportionate to grant it for one of the statutory purposes, despite the invasion of privacy that was likely to be involved, and that the justification for the warrant persists if it remains extant. I also check the paperwork to ensure that it is complete, that warrants have been renewed in time, and have been cancelled when no longer justifiable. As last year I have set out in Table 2 the stages and purposes of a typical inspection visit.

Table 2 – An Inspection Visit

Stage	Description	Purpose
Selection Stage	Warrant-Issuing Department (WID), Intelligence Agency or Law Enforcement Agency (LEA) provide list of extant, expired and modifications to authorisations since last inspection.	Checks are made by WID to ensure all authorisations are submitted.
	Agencies also commonly refer commissioner to specific cases of interest concerning either errors or legal issues.	
	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 (up to 1 month later)	Brief by senior officials on threat and emerging policy issues. Reading through and scrutinising authorisations. Pre-reading time can be set aside to ensure commissioner has had time to review all paperwork related to authorisations prior to inspection visit. Where necessary, oral briefings by case officers to detail intelligence case behind the submissions and answer commissioner's questions on any errors.	To provide commissioner with a general operational overview as to the nature of the threat in relation to which applications for authorisations may be sought. Commissioner seeks to reassure himself that throughout authorisation process principles of necessity, proportionality and other safeguards have been applied. Specific focus on ensuring renewals are being submitted in good time and that urgent oral applications really are urgent.
Follow-up stage	Meetings with Secretary of State. Report of Inspections within Annual Report. Potential informal consultation between agency and commissioner on challenging legal or policy issues. Discussions with officials at Department of State through whom submissions go before reaching Secretary of State.	Ensure getting best value from commissioners' expertise. Characteristic of an effective relationship between commissioner and Agencies.

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 Code 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 important to ensure that the facts justified the use of interception, and that the principles of necessity and proportionality have been adhered to.

Throughout my 2011 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 lawful 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 being approved in my opinion remains very low due to the high level of scrutiny that is applied to each authorisation as it crosses a number of desks in the corresponding warrantry units of the Home Office, Foreign Office, Ministry of Defence, Northern Ireland Office and Scottish Office, before reaching the relevant Secretary of State or Scottish Minister.

6.3 Lawful Intercept Warrants

In previous reports I have presented the following:

- Number of lawful interception warrants signed by the Home Secretary (for national security and serious crime) both in-year and extant at the year-end.
- Number of modifications to lawful interception warrants authorised by a Senior Official at the Home Office both in-year and extant at the year-end.
- Number of lawful interception warrants signed by Scottish Ministers both in-year and extant at the year-end.
- Number of modifications signed by Scottish Senior Official both in-year and extant at the year-end.

My rationale for presenting these figures has been to illustrate to readers the extent to which lawful interception was being used as a tool to counter the problems faced by the UK arising from serious crime, and threats to national security. In last year's annual report I was able to present year-on-year changes in warrant numbers.

I have also set out in previous reports that the Foreign Secretary (on behalf of SIS and GCHQ), the Defence Secretary and the Secretary of State for Northern Ireland authorised applications for lawful interception. However, I did not disclose the numbers of such warrants in the open report as I accepted that doing so might have undermined national security. My position in relation to warrants signed by the Home Secretary was that as the total number included both warrants issued in the interest of national security, and for the prevention and detection of serious crime, disclosure of this combined figure did not undermine national security.

During a period of potential reform to intelligence oversight, driven in part by demands for greater transparency about the extent of commissioner oversight, I have reconsidered with the security services and others the reasoning behind the non-disclosure of warrant numbers in relation to those Departments previously omitted from the open report. The objective of the exercise has been to seek to develop a method of illustrating the quantum of interception warrants signed in the UK and from which I could sample during inspection visits.

I present in this section therefore, the results of the discussions with those public authorities whose lawful interception activities I oversee. I am able this year to report a single figure comprising the total number of lawful interception warrants signed by the Secretaries of State and the Scottish Ministers. This figure fulfils the objective of enabling readers to discern the total pool of warrants from which I select my samples for review during Inspection visits whilst not disclosing information, for example on the extent of coverage of any specific target that may be detrimental to national security.

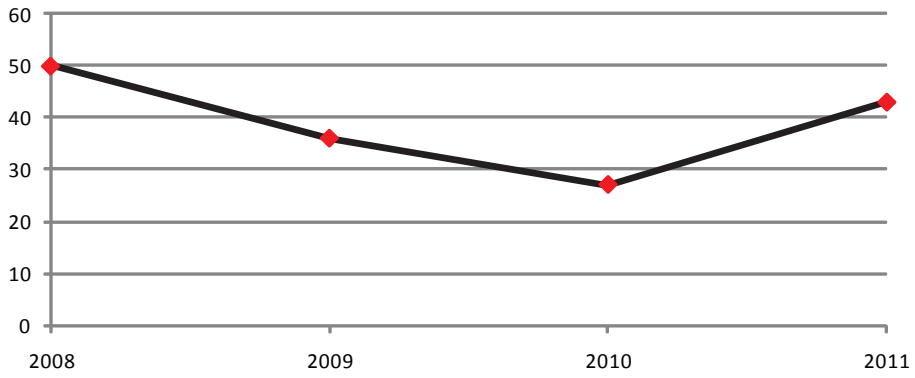
The total number of lawful intercept warrants issued in 2011 under Part I Chapter I of RIPA therefore was 2911.

I do not record the number of warrants which I have examined in relation to each agency because to do so would be of little value. In relation to some agencies I see most if not all of the warrants, but where the number of warrants is large I have to select. I usually select operations rather than warrants. Often one operation will generate a host of warrants and renewals. For example, one SOCA operation I looked at recently generated over 60 warrants, and of course I may see some of the same warrants when I inspect the warrants held by the Departments of State. But I have had the benefit of statistical advice to satisfy myself that, even when the pool of warrants is large, the numbers that I examine are statistically relevant.

It is important to note, as set out in the previous section, that the power to grant an interception warrant rests only with a Secretary of State or his Scottish equivalent, who must be persuaded that the warrant is necessary for the pursuit of the public authority objective and proportionate to what it seeks to achieve. The lawful interception of communications remains, in my view, a valuable tool against those who seek to harm the UK through committing serious crime, threatening national security or seeking to harm the nation's economic well-being.

6.4. Errors Across all Lawful Intercepting Agencies

Figure 2 – Total Number of Intercept Errors over the previous 4 years



42 errors have been reported to me during the course of 2011. Although this represents a significant increase on the 27 errors reported in 2010, which is regrettable, the number of reported errors represents 1.4 % of the total number of lawful intercept warrants signed in 2011.

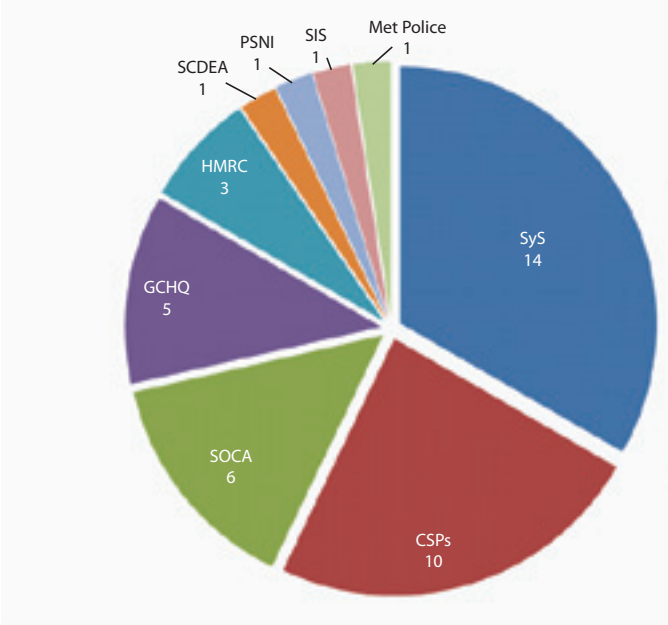
Despite the increase in the number of errors, I am satisfied that none of the reported errors or breaches were deliberate. There were two causes of errors; human and technical. Typical human errors were:

- transpositions of numbers, or incorrect recording of communications addresses
- failing, because of staff changes, to renew a warrant when it lapsed

Technical or software problems occasionally caused errors which could be system-wide.

In every case where an error occurred, either no interception took place, or the product was destroyed and steps were taken to reduce the risk of repetition. Sometimes, depending on the nature of the error, staff had to receive further training or guidance. Sometimes systems had to be revised or technical problems had to be analysed and eliminated.

Figure 3 – 2011 Breakdown of Intercept Errors by Agency



6.5. Inspection Results

This section deals with the outcomes of those inspections that I undertook in 2011, in relation to lawful interception under Part I, Chapter 1 of RIPA. I set out details of briefings I received during each inspection visit, those whom I met, in broad terms what was discussed, and, my assessment of compliance at each agency or department I oversee. In addition I set out details of some of the errors that occurred, to the extent I am able to disclose without detriment to national security.

6.5.1. GCHQ

In relation to GCHQ, lists of relevant material were sent to my office in May and November 2011. My formal inspection visits to GCHQ were in late June and December respectively. I selected a number of warrants of varied types for review during the formal oversight visit. All inspection visits took place at GCHQ in Cheltenham.

During my inspection visits I met the Director of GCHQ and the Director-General for Intelligence and Strategy. They briefed me as to the current level of threat. I then scrutinised the selected warrants, with the assistance of the relevant case officers, and discussed with GCHQ lawyers and other senior members of staff matters to which they wished to draw my attention.

During December 2011 I spoke to many of the local compliance staff on my role as commissioner, which was followed by a Question and Answer session about the role of legalities in relation to GCHQ operations. In addition, GCHQ legal advisers have taken the opportunity to discuss

emerging capabilities with me outside the inspection visits.

Once again, it is my belief, based on my scrutiny of GCHQ authorisations, in addition to what I have seen at both Inspection visits and wider briefings, that GCHQ staff conduct themselves with the highest levels of integrity and legal compliance.

Case Study 4 – Example of an Intercept Error by GCHQ

January 2011 - GCHQ holds a long-running interception warrant against a target organisation. In 2009, an analyst from the relevant team entered a communications address onto a targeting database. The address had not, however, been listed on the schedule to the relevant interception warrant. The anomaly was detected when a manager undertook a regular house-keeping check on all communications addresses covered by the warrant. The number was immediately de-tasked and an investigation initiated into any wider discrepancies between targeting records and authorised communications addresses on warrants. No intelligence reports were issued based on material incorrectly intercepted.

6.5.2. Security Service (SyS)

Key periods related to my inspection visits to SyS over 2011 were as follows

Selection: June and November 2011

Inspection Days: July and December 2011

During my formal Inspection visits to SyS, I was briefed on the following.

- International Counter-terrorism threats
- State-led threats
- Northern Ireland Related Terrorism (NIRT)
- Presentations related to specific interception warrants
- Olympics planning

Below are two case studies of instances where the SyS erred.

Case Study 5 –Example of an Intercept Error by the SyS

March 2011 – Following a fault in the CSP's interception system, the service worked with the CSP to mitigate the consequential loss of intelligence collection and threat to national security as a result. Due to a breakdown in internal communications the solution for the interception of an internet connection did not take into account undertakings made in the corresponding warrant application regarding how the intercepted material would be handled; intercepted material was no longer subjected by the Security Service to handling arrangements that were required by the warrant and had been previously applied. A number of new measures and procedures were established to minimise the risk of the error being repeated. The error was reported to the Commissioner who was content with the detailed report and measures outline to minimise the risk of any repetition.

Case Study 6 – Example of an Intercept Error by the SyS

September 2011 - An error occurred in relation to the transcription of communications which did not adhere to the undertakings set out in a warrant. A warrant authorising interception of a target communications line was signed. The warrant specified that only certain types of call would be transcribed and retained. Human error resulted in some communications outside of the parameters set out in the warrant being transcribed. As a follow up action staff were reminded of the importance of fully understanding their transcription briefs prior to commencing work on target lines.

6.5.3. Secret Intelligence Service (SIS)

The chronology of my scrutiny visits to SIS over 2011 was as follows:

Selection Days: May and November 2011

Inspection Days: late May and early December 2011

All inspections were held at SIS HQ, Vauxhall Cross, London.

I believe that scrutiny of those interception warrants selected, combined with the level of discussion I was able to have with a cross-section of staff on the subject of legalities during my Inspection and wider briefing visits is sufficient for me to conclude that compliance at SIS was robust. I was again impressed by the attitude of all those that I have spoken who work for SIS.

I discussed the following during my inspection visits:

- Threat briefing
- RIPA interception warrants

Once again, I was satisfied that officers working for the SIS conduct themselves in accordance with high levels of ethical and legal compliance.

6.5.4. SOCA, HMRC, PSNI, Metropolitan Police and Scottish Government

I have followed the practice of previous years and visited the following Departments on two occasions in 2011 to undertake warrantry reviews

Department	Selection Periods	Inspection Periods
Serious Organised Crime Agency (SOCA)	mid June mid November	mid July early December
Police Service Northern Ireland (PSNI)	May November	early June late November
Her Majesty's Revenue and Customs (HMRC)	early July early November	late July early December
Metropolitan Police Counter-Terrorism Command (MetCTC)	early June early December	late June late December
Scottish Government	early July mid November	late July early December

Matters related to HMRC, Met CTC, PSNI and SOCA were discussed during meetings with respective Secretaries of State and I took the opportunity to discuss Scottish Government business with the Scottish Cabinet Secretary for Justice. When I met him in December 2011 he expressed satisfaction in relation to the information he received to support the warrant applications he considered. From this meeting and my bi-annual reviews, I was able to form the impression that the staff involved in the preparation and execution of warrantry in Scotland, were diligent and fully aware of their obligations in relation to the legislation.

Case Study 7 – An Example of an Intercept Error by SOCA

March and July 2011 - SOCA reported two breaches where incorrect information regarding the attribution of communications addresses had been provided by operational teams to technical staff. The cause of both errors was human oversight, first in relation to keying error, second the misattribution of a digit. The errors were immediately identified and the communications addresses deleted from systems. In each case the operational teams were advised of the errors and of the importance of double-checking the accuracy of numbers before providing them to warrantry and ultimately technical staff to be placed under intercept.

Case Study 8 – An Example of an Intercept Error by the Metropolitan Police

May 2011 - The reported error concerned the transposition of a digit in relation to a mobile phone to be placed under interception. Interception commenced and the breach was immediately identified, at which point all activity was suspended. Met CTC applied for a new schedule to be added to the warrant with the correct communications address. At this point interception recommenced. More stringent quality assurance processes were implemented by the agency to prevent this kind of breach recurring. A new post of Head of Warrantry was additionally created at the agency to manage intercept warrant applications more effectively.

Case Study 9 – An Example of an Intercept Error by HMRC

January 2011 - The error related to preparatory work prior to the drafting of a new warrant application for a large scale fraud investigation. The incorrect provision/mechanism under RIPA was used to obtain data in relation to communications devices. The numbers were obtained directly from operational teams. Once the error was identified the warrant applications were suspended and a series of remedial measures were taken. These included the officer concerned being reprimanded and reminded of his obligation to adhere to the correct legislation and guidelines. Furthermore all staff were reminded verbally and in writing about their legal responsibilities and the incident was incorporated as a case study into training packages for new staff.

6.5.5. Communication Service Providers (CSPs)

I have continued the practice as in previous years of making informal annual visits to communications service providers (CSPs). These meetings, not required by the legislation, are again reflective of the good relationships between the CSPs, the intelligence community and myself.

The purpose of these visits, many of which take place out of London, has been for me to meet on an informal basis senior staff and individuals engaged in lawful interception, in order to be briefed on changes to technology and work relationships between the intercepting agencies and CSPs. The staff within CSPs welcome these visits and the opportunity to discuss with me their work, the 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.

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 the 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.

Case Study 10 – An Example of an Intercept Error by a CSP

February 2011 - A CSP was tasked by an intelligence agency to provide information authorised for collection in relation to a warranted target. This involved the co-ordination of two collection systems at the CSP. Due to digit transposition the details of an existing target were used, and additional information was gathered in relation to the existing target. The agency therefore received unauthorised information in relation to an existing target. The error was immediately identified and rectified. Steps were then taken to prevent a recurrence, which included ensuring staff were made aware of the importance of ensuring that numbers are checked and re-checked in relation to interception targets.

Case Study 11 - An Example of an Intercept Error by a CSP

September 2011 - A CSP reported an error as a result of which interception was targeted at an uninvolved third-party. The usual processes in place to prevent incorrect targeting had been ineffective in noticing or preventing the initial operator error. The cause of the error was human oversight. An operator incorrectly recorded a communications address at the feasibility stage and then failed to check back with relevant systems to ensure that the correct tasking was being undertaken. The error was discovered some days later as part of a routine call back to the requesting agency. The disparity between the paperwork and intercept systems was noted. The error was immediately rectified. Any product collected was destroyed. A number of steps were taken to reduce the likelihood of recurrence. The CSP has now implemented a system involving a second person checking each new tasking to ensure accuracy. Daily checks have also been expanded to ensure that tasking registers and intercept systems match up.

6.5.6. Home Office

Security Service and law enforcement interception warrants must pass through the National Security Unit at the Home Office prior to reaching the Home Secretary. I have undertaken inspection visits to the Home Office as an extra check on authorisations. I undertook formal visits to the Home Office in June and December. Lists of interception warrants (current, extant and expired) were provided to my office in good time to select sample warrants for these review visits. The visits took place in the Home Office, London.

Meeting with Home Secretary

I met with the Home Secretary in early 2012. We discussed in broad terms, whether she felt she was being supplied with sufficient information when signing interception warrants for national security and serious crime, my views on the agencies' compliance with RIPA, some specific errors I was concerned with, the structure of my forthcoming Annual Report, non-statutory compliance and other relevant policy matters. These matters are discussed in more detail in the confidential supplement that accompanies this report and will be distributed to senior intelligence officials across Whitehall.

I am satisfied that the Home Secretary takes care before signing interception warrants that potentially infringe on the private lives of citizens. It was apparent that she took time to read submissions throughout the day, often requesting further information and updates from officials in relation to certain warrants. The Secretary of State does not 'rubber-stamp' authorisations.

6.5.7. Foreign and Commonwealth Office (FCO)

I also undertake inspection visits to the FCO. The purpose of these visits is to meet with those senior officials at the Department of State (Head of Intelligence Policy Department, Director of National Security and Director-General Defence and Intelligence) who advise the Secretary of State on matters related to his signing of GCHQ and SIS authorisations. I also undertake an additional scrutiny of SIS and GCHQ warrantry submissions.

For the purposes of this scrutiny I select in advance from the lists of current and cancelled warrants supplied by the FCO. My selection may include some warrants already examined, or to be examined, at agency inspections as well as other warrants not reviewed elsewhere.

In relation to the FCO, lists of relevant material were sent to my office in May and November 2011. My formal inspection visits were held in early June and December respectively. Once again, I was satisfied with both the information provided to me at the FCO and the levels of oversight and compliance shown by those officials I met.

Meeting with Foreign Secretary

I met with the Foreign Secretary in mid December to discuss the discharge of my oversight role in relation to the intelligence agencies (GCHQ and SIS) for whom he is responsible. In broad terms we were able to have a fruitful discussion on agency compliance with RIPA, and he gave his views on the level and depth of information within submissions he signs. We were also able to discuss the proposed structure of my annual report, the Justice and Security Green Paper and other policy matters. It was clear from this meeting that the Foreign Secretary takes very seriously his responsibilities for authorising interception applications from SIS and GCHQ.

6.5.8. Ministry of Defence

My formal inspection visits at MoD took place in late June and late November. I was able to scrutinise the MoD interception warrants and was satisfied that they were properly authorised and up-to-date. I was also briefed in-depth on the basis of these warrants during a visit to the Defence Science and Technical Laboratory (DSTL) in Porton Down in August 2011.

6.5.9. Northern Ireland Office (NIO)

As part of my oversight function I also visit the Northern Ireland Office in order to inspect lawful intercept warrants signed by the Secretary of State for Northern Ireland. In relation to the NIO, lists of relevant material were sent to my office in May and November. My formal inspection visits took place in early June and late November.

In broad terms I was briefed on the following during the inspection visits

- Policy and legal matters in relation to selected warrants
- National security and political update from senior NIO officials
- Broad interception techniques
- Errors reported to me in the preceding six month period

Meeting with Secretary of State for Northern Ireland

I met with the Northern Ireland Secretary in mid November 2011. We covered a wide range of topics during the discussion, including NI political and security situation, his assessment of the quality of authorisations submitted to him for signature, Olympics planning, my annual report and whether there were occasions when he refused to sign authorisations. It was clear to me that the Secretary of State took his responsibilities for authorising potentially intrusive acts seriously.

Although outright refusal to sign authorisations was rare, the Secretary of State did on occasions send submissions back for further information. I was also pleased to hear from others the extent to which the Secretary of State was willing to be contacted by staff out of hours to seek oral authorisations in particularly urgent and important cases when a physical authorisation was not possible.

6.6. Summary of Lawful Intercept Compliance

It is my view, based on the range of checks I undertake as commissioner, that those agencies and departments which I oversee are compliant with the legislation. I have observed, both this year and during previous years, that questions concerning the strength of the intelligence case, compliance with legalities and ethics are posed at every stage of the warrant application process. Through my meetings with officers involved in interception, in addition to Secretaries of State and Scottish Ministers, I am able to form the view that all those involved act with integrity and in a highly ethical manner.

That is not to say errors cannot occur during complex investigations involving the co-ordination of the interception process across many agencies. The number of errors reported to me has increased from 27 in 2010 to 42 in 2011. The in-depth nature of error reports I have received during the year, supported when necessary by in-depth explanations during inspections, allows me to conclude that none of the errors reported were malicious or deliberate. Each error involved some kind of human error or system-related problem. I have been assured that any intelligence obtained through erroneous means was destroyed.

Any increase in errors is regrettable and I have stressed to those involved the importance of reminding staff of the need to comply with the legislation and to reform procedures where necessary to minimise the risk of errors being repeated in the future.

7. COMMUNICATIONS DATA (RIPA PART I, CHAPTER II)

7.1. General Background to Types of Communications Data

There are three types of communications data gathered under RIPA Part I, Chapter II. These are fully defined in RIPA but in summary;

- Subscriber Data relates to information held or obtained by a Communications Service Provider (CSP) in relation to a customer (e.g. name and address of account holder of an email address).
- Service Use Data is information relating to the use made by any person of a communications service (e.g. itemised telephone call records showing the date/time and duration of calls made and the numbers dialled).
- Traffic Data is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication (e.g. anything written on the outside of a postal item concerning its postal routing).

Certain public authorities are approved by Parliament to acquire communications data, under Part I, Chapter II 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.

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.

7.2 Inspection Regime

I am supported by a Chief Inspector and five inspectors who are all highly trained in the acquisition and disclosure criteria, processes and the extent to which communications data may assist public authorities in carrying out their functions. My inspection team, supported by two administrative staff, undertake a revolving programme of inspection visits to public authorities who are authorised to acquire communications data. The inspections take between 1 and 5 days, depending on the level of access the public authority has been granted under the Act, how frequently they are using their powers to acquire communications data and their previous level of compliance.

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.

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 Part I, Chapter II of RIPA and its associated Code of Practice.
- Provide independent oversight of the process and check that the matter under investigation was such as to render the acquisition of data necessary and proportionate.
- 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.

At the start of the inspections my inspectors review any action points and recommendations from the previous inspection to check that 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.

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.

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.

My inspectorate receives good co-operation 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.

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 some more examples of how communications data has been used effectively by public authorities to investigate criminal offences.

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.

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 traffic light system (red, amber, green) has been adopted for the recommendations to enable public authorities to prioritise the areas where remedial action is necessary. Any red recommendations are of immediate concern as they mainly involve serious breaches and/or non-compliance with the Act or Code of Practice which could leave the public authority vulnerable to challenge. The amber recommendations represent non-compliance to a lesser extent; however remedial action must still be taken in these areas as they could potentially lead to serious breaches. The green recommendations represent good practice or areas where the efficiency and effectiveness of the process could be improved. 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.

7.3. Communications Data Requests

During the reporting year public authorities as a whole, submitted 494,078 requests for communications data. The intelligence agencies, police forces and other law enforcement agencies are still the principal users of communications data. It is important to recognise that public authorities often make many requests for communications data in the course of a single investigation, so the total figure does not indicate the number of individuals or addresses targeted. Those numbers are not readily available, but would be much smaller. Figure 4 illustrates that the number of requests submitted in 2011 represents an 11% decrease on the previous year. The statistics my office have collated show that 29 police forces have reduced their demands for communications data on the previous year. The following explanations for the reduction in usage have been provided by some of these police forces; the conclusion of a number of

long running investigations where communications data was pivotal in 2010, a reduction in the number of major enquiries, and, budgetary restraints. It is noticeable that the number of requests for 'combinations' of data falling under Sections 21(4)(a), (b) and (c) have increased (as described in the next paragraph of this report) and this has also contributed to reducing the overall number of requests.

Figure 4 – Number of Notices/Authorisations for Communications Data in the Previous 4 Year Period

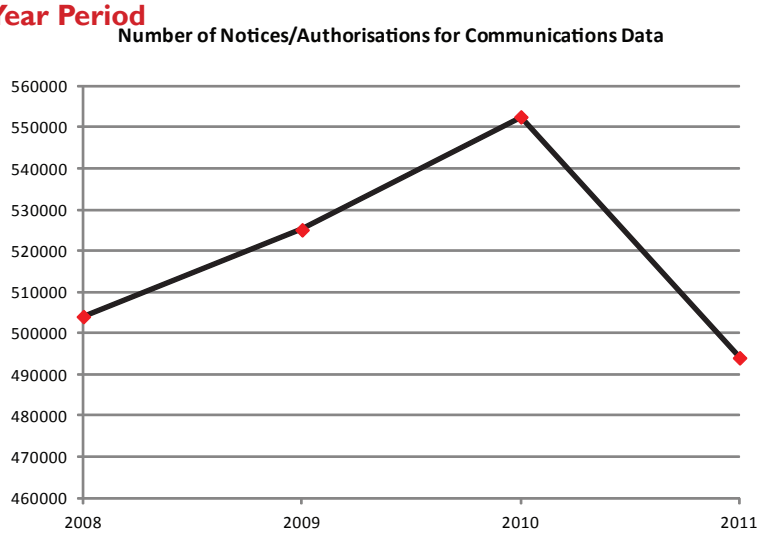
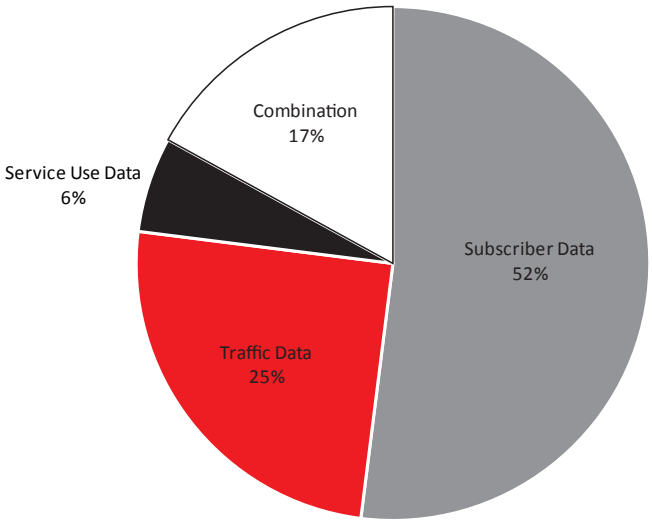
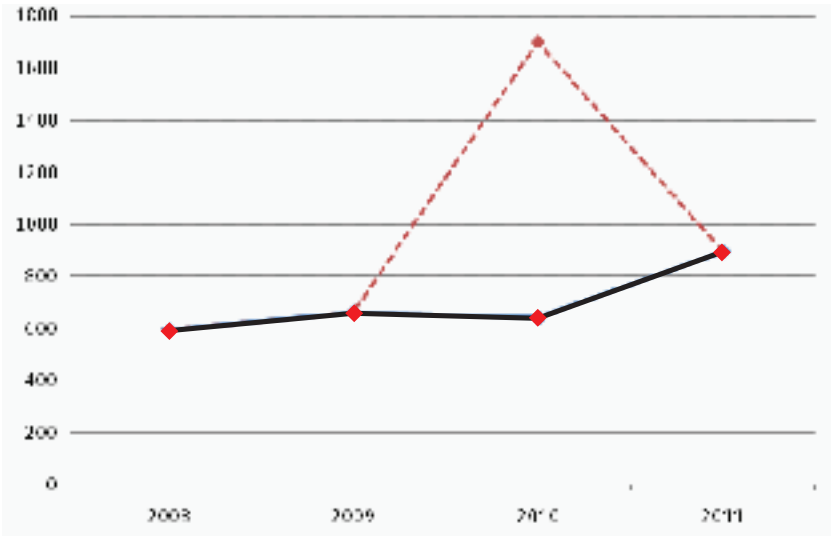


Figure 5 – Breakdown of Communications Data Authorisations/Notices by Type



7.4. Communications Data Errors

Figure 6 - Number of Communications Data Errors Reported to the Commissioner in the Previous 4 Years



During the reporting year, 895 communications data errors were reported to my office by public authorities. This figure is higher than the previous year (640). However, in 2010 an additional 1061 errors were also reported to my office and these, although kept separate from the 640 figure for reasons I outlined in my previous report, were included in the overall error percentage. Therefore the overall error percentage has actually reduced from 0.3% in 2010 to 0.18% in 2011. I am satisfied that the overall error rate is still low when compared to the number of requests that were made during the course of the reporting year.

Approximately 80% of the 895 errors were attributable to public authorities and 20% to CSPs. This year my office has collated management information in relation to the causes of the errors and as a result I am able to provide more detail in this area. Figure 7 illustrates the breakdown of errors by cause.

Figure 7 – Breakdown of Errors by Cause and Responsible Party

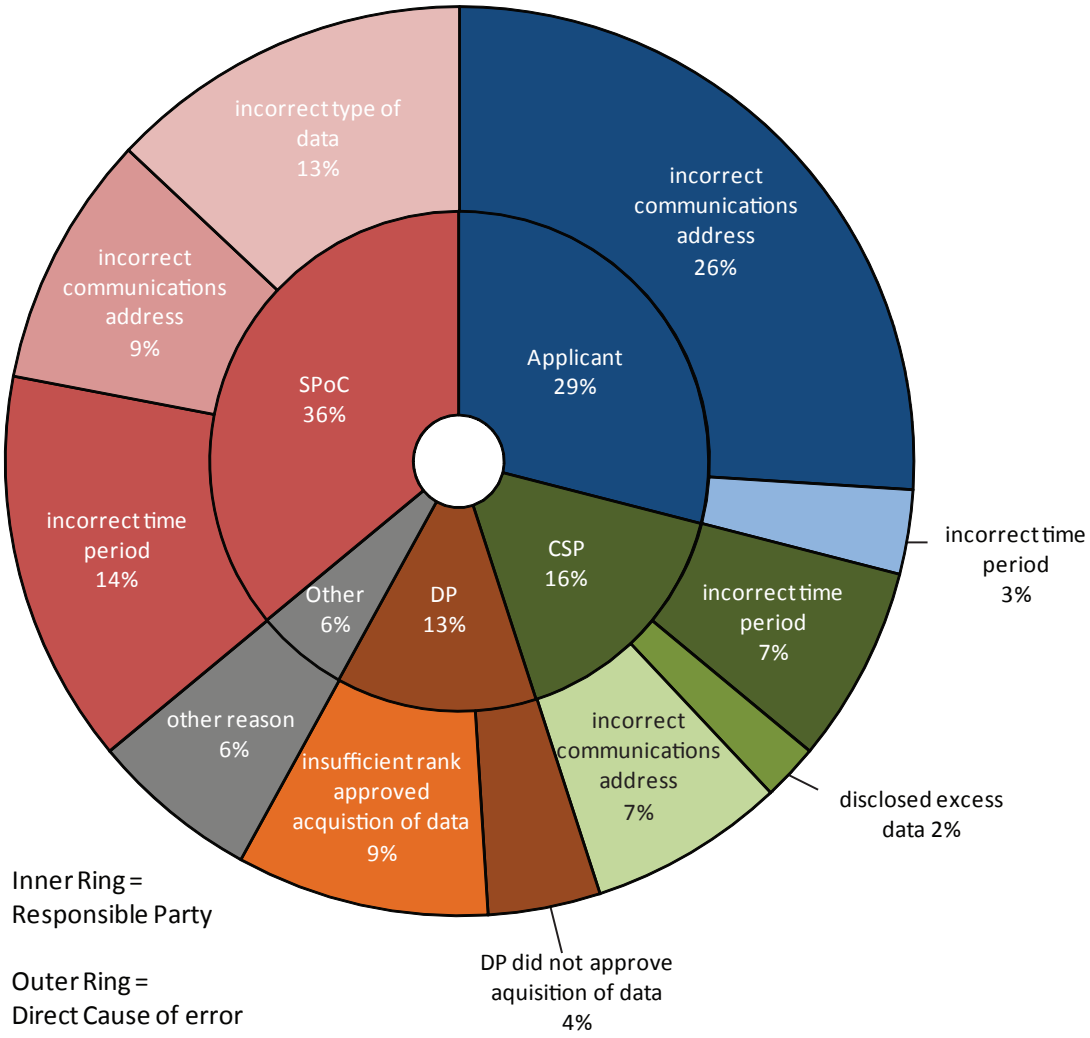


Figure 7 shows that 42% of the errors were caused either by the applicant, SPoC or CSP acquiring data on the incorrect communications address. This type of human error usually occurs due to the transposition of digits in telephone numbers or internet protocol (IP) addresses. In the vast majority of these cases the mistake was realised, the public authority (and CSP if applicable) reported the error to my team and the data that was acquired wrongly was destroyed as it had no relevance to the investigation. Unfortunately in two separate cases where a CSP disclosed the incorrect data, the mistakes were not realised and action was taken by the police forces on the data received. Regrettably, these errors had very significant consequences for two members of the public who were wrongly detained / accused of crimes as a result of the errors. I cannot say more about these two instances at this time as investigations are ongoing. However when such errors occur it is my responsibility to investigate the circumstances and work with the CSP or public authority concerned to review their systems and processes to prevent any recurrence. In these cases the CSP was slow to report the errors and I was not initially satisfied with the explanations the CSP provided in relation to how the errors occurred, or the measures they put

in place to prevent recurrence. I am pleased to say that this CSP has since put in place some very sensible measures which will hopefully prevent recurrence of similar errors in future. Fortunately errors with such severe consequences are rare.

Figure 7 shows that 24% of the errors were caused by either the applicant, SPoC or CSP acquiring data on the correct communications address but for the incorrect date / time period. An additional 13% of the errors were caused by the SPoC acquiring the incorrect type of data (i.e. outgoing call data instead of subscriber data) on the correct communications address.

The vast majority of the errors I have described in the preceding paragraphs could be eradicated by removing the double keying in the systems and processes. However in 26% of cases the process started with the applicant actually requesting the incorrect details and this demonstrates the need to emphasise the importance of double checking to applicants.

I will provide further information in relation to some of these errors later in this report. However it is worth mentioning now that 99 of the 895 errors were identified by my inspectors during the inspections. This confirms that the inspections are worthwhile and provides evidence that the public authorities' records are properly scrutinised by my inspectors. In the main these errors had not been reported by the public authorities in question as they had genuinely not realised they had occurred. In a very small number of cases the lack of reporting was an oversight.

Under the Code of Practice I have the power to direct a public authority to provide information to an individual who has been adversely affected by any wilful or reckless exercise of or failure to exercise its powers under the Act. So far it has not been necessary for me to use this power but there is no room for complacency, and each public authority understands that it must strive to achieve the highest possible standards.

7.5. Inspection Results

As already indicated a team of inspectors, lead by a Chief Inspector, inspect on my behalf those public authorities with the requisite powers under RIPA to acquire communications data. Due to the larger number of public authorities with powers to acquire communications data, the presentation of the results of communications data inspections differs from the presentation of the results of the inspections I conduct in relation to lawful interception. The bodies being inspected fall into 4 groups: police forces and law enforcement agencies (LEAs), intelligence agencies, local authorities, and 'other' public authorities. I now set out the key findings of the inspections in relation to these groups, along with some further case studies where communications data has been used effectively in investigations.

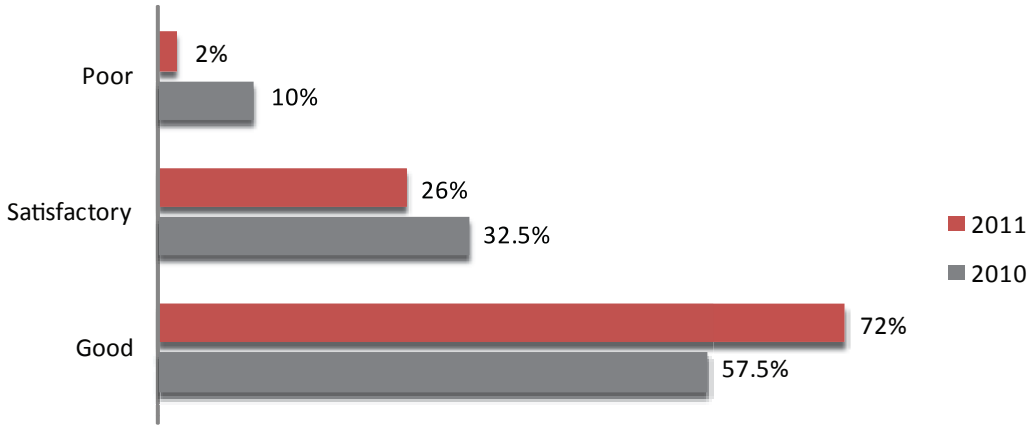
7.5.1. Police Forces and Law Enforcement Agencies

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 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).

In 2011 my inspection team conducted 43 inspections of police forces and law enforcement agencies. Generally the outcomes of the inspections were good, and the inspectors concluded that communications data was being obtained lawfully and for a correct statutory purpose. Figure 8 illustrates that 72% of the police forces and law enforcement agencies achieved a good level of compliance overall. This represents a 14.5% increase on the previous year. However this percentage should be treated with caution as the public authorities being inspected are not the same every year.

Figure 8 – Comparison of Police Force and LEA Inspection Results, 2010 vs. 2011



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 had either improved or sustained their good level of compliance with the Act and Code of Practice. The four police forces and law enforcement agencies that emerged poorly from their 2010 inspections were revisited in 2011 to ensure that they had improved their standards. I am pleased to report that they had all worked hard to achieve their recommendations and that three emerged from their 2011 inspections with a good level of compliance. The remaining one emerged with a satisfactory level of compliance.

> *"The vast majority of police forces and law enforcement agencies had fully implemented their previous recommendations. As a consequence, an overwhelming number had either improved or sustained their good level of compliance with the Act and Code of Practice"*

In fact only one police force emerged poorly from their 2011 inspection and I am pleased to report that this public authority has already been re-inspected and is now achieving a good level of compliance.

All of the police forces and law enforcement agencies that were inspected during the reporting year were consistently producing good or satisfactory quality applications. This is an improvement on the previous year and it is clear that the applicants are more accustomed to the process. My inspectors were satisfied that the acquisition of the data was necessary and proportionate. There is evidence that the SPoCs are adopting a more robust guardian and gatekeeper function and they are providing good advice to applicants to assist them to meet the requirements.

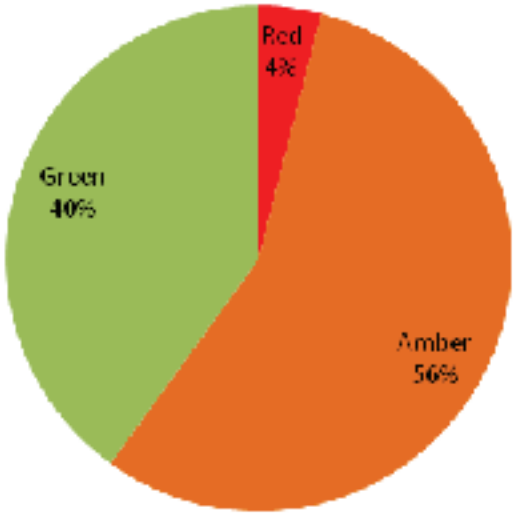
A number of CSP disclosures were randomly checked against the records kept by the police forces and law enforcement agencies, and I am pleased to say that in all cases my inspectors were satisfied the correct process had been applied and the data had been obtained with the approval of a DP. I regard 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.

My inspectors concluded that the DPs are generally discharging their statutory duties responsibly. The DPs in 88% 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. The statistics provided to my office this year indicate that over 6,000 applications were rejected in 2011 by DPs in police forces and LEAs. I cannot give this figure as a percentage because the total number of applications is not reported to me. My inspectors also concluded that there is more objectivity and independence in the approvals process within specialist departments such as Special Branch (SB) and Professional Standards Departments (PSDs), or alternatively, they found that Paragraph 3.11 of the Code of Practice is being complied with. Last year I reported that this was an area where there were compliance and quality issues and therefore it was pleasing to find such a good level of compliance in this round of inspections.

"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. The statistics provided to my office this year indicate that over 6,000 applications were rejected in 2011 by DPs in police forces and LEAs"

I outlined earlier in this report that a traffic light system (red, amber, green) has been adopted for the recommendations that emanate from the inspections. This enables public authorities to prioritise the areas where remedial action is necessary. This year 282 recommendations were made by my inspectors during the 43 law enforcement agency inspections, which is an average of 6 recommendations per public authority. Figure 9 shows the breakdown of recommendations by colour.

Figure 9 – Recommendations from 2011 Police Force and LEA Inspections



I am pleased to report that only 4% of the recommendations represented serious non-compliance with the Act and Code of Practice. These recommendations fitted into two distinct areas; the urgent oral process and the procedures surrounding the acquisition of 'related' communications data.

"Only 4% of the recommendations represented serious non-compliance with the Act and Code of Practice. These recommendations fitted into two distinct areas"

First, in relation to the urgent oral process, my inspectors found evidence of DPs in three police forces giving a 'blanket' or 'rolling' authority at the start of immediate threat to life incidents to obtain any data necessary. In these cases the DPs had not given the requisite authority for the subsequent data that was acquired to be obtained. In another case where the DP had given specific approval for certain data to be obtained, the SPoC went on to acquire data in addition to that which was originally approved, without obtaining further approval from a DP. Although these instances represent serious non-compliance, I am satisfied that they were not wilful or reckless failures. It is also important to recognise that they occurred in relation to exceptionally urgent cases and that the persons involved in the process were working under immense pressure in an attempt to save lives. Nevertheless, it is still important to ensure that the correct process is always applied and that the data is acquired in accordance with the law.

Second, my inspectors found that a number of police forces and law enforcement agencies had misunderstood the procedures for acquiring communications data based on lawful intercept product and as a result the proper application process had not been followed. However, in these cases the communications data that was acquired was approved by a DP in all instances and the inspectors were satisfied that the requests were necessary and proportionate.

The SPoC has an important responsibility under the Code of Practice to make sure the public authority acts in an informed and lawful manner. In my last annual report I said that it is vitally important for public authorities to have the right number of well trained staff in this business area. I am therefore concerned that my inspectors found that 20% of the police force and law enforcement agencies inspected in this reporting year had a lack of staff in their SPoC. These authorities were experiencing serious backlogs in dealing with applications, and the systems and processes were not being managed efficiently or effectively. There is a risk in these cases 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.

"20% of the police force and law enforcement agencies inspected in this reporting year had a lack of staff in their SPoC"

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 35,109 requests were orally approved which represents an increase on last year's figure of 31,210. Again marked improvements were found in the management of the urgent oral process and the quality of the record keeping, with 90% of the police forces and law enforcement agencies now achieving a good or satisfactory standard in this area, save for the errors I have already outlined.

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. This year inspections were conducted in two regions where police forces had brigaded their SPoC resources. 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.

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 two 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 two examples are based on extracts from the inspector's reports.

Case Study 12 - Cambridgeshire Constabulary

Cambridgeshire Constabulary used communications data to good effect during Operation Gritstone, an investigation into aggravated burglary. The brief circumstances of the case are that two men attempted to force their way into a residential premises with the intention of stealing cash and drugs. A friend of the homeowner barred their way and in the ensuing struggle he was shot with a sawn off shotgun, receiving serious wounds. A fingerprint from the scene identified a suspect from the Northampton area and two of his known associates subsequently became suspects. Mobile telephones were identified for the three suspects and a communications data strategy was devised. Initially subscriber checks and call data was acquired to attribute the phones to the suspects. Location data was then acquired and the analytical work showed that all 3 suspects travelled together from Northampton to Cambridgeshire and then back to Northampton shortly after the offence. The location data led the police to recover CCTV footage from close to the crime scene which provided evidence of the suspects association to a vehicle that was later seen by a witness around the time of the shooting. Communications data that was acquired as part of the investigation also crucially led to the arrest of one of the suspects. All three suspects were charged with possession of a firearm, grievous bodily harm and aggravated burglary. The defendant who discharged the firearm pleaded guilty at Peterborough Crown Court and was sentenced to 7½ years imprisonment. The other two defendants, one of whom acted as the getaway driver, elected for a trial and in April 2011 they were convicted on all counts. They were sentenced to 8 and 13 years imprisonment.

Case Study 13 – Northern Constabulary

Northern Constabulary used communications data very effectively during an investigation into housebreaking and indecent assault of an elderly widow who lived alone in Alness, near Inverness. The investigation team started by developing intelligence and research on known sex offenders with similar modus operandi. Analysis of communications data acquired in relation to one of these suspects actually served to eliminate him from the enquiry. Further enquires identified that Central Scotland Police were investigating a similar attack on an elderly female and had released a Crime Bulletin for information on a suspect. Following liaison between the Scottish Forces it was established that this suspect may also have committed similar attacks on elderly females in the Kilmarnock area. The suspect was also sought by police from Lincolnshire as he had been convicted in his absence of a similar offence in 2007 and was suspected of committing a further offence in August 2010. Northern Constabulary took the lead in pursuing the communications data strategy and a mobile phone number was identified for the suspect. Communications data was initially acquired on this number using the urgent oral process as there was an urgent operational requirement to arrest the suspect. This data indicated that the phone was roaming abroad, and further intelligence and financial enquiries indicated that the suspect was in the Republic of Ireland. The suspect was arrested on his return to Scotland. Further applications for communications data requested subscriber / account information, incoming and outgoing call data and location data on the suspect's mobile telephone. The data was requested for periods of time covering the four crimes and in the period leading up to the suspect's arrest. The data acquired was analysed and clearly linked the suspect to the offences. Ultimately the data provided a vital contribution to the evidence presented at the trial and the defendant was convicted of house breaking, assault and theft.

At Edinburgh High Court the defendant was sentenced to 10 years imprisonment and was issued with a lifelong restriction order.

7.5.2. Intelligence Agencies

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.

During the reporting year all three of the intelligence agencies were inspected (Sys, SIS, GCHQ). My inspectors were satisfied that the agencies are 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 requests are necessary and proportionate. The DPs are discharging their statutory duties responsibly and the SPoCs are ensuring the data is acquired in a timely manner. The inspections at GCHQ and SIS did identify a number of areas where their systems could be updated to streamline the processes and reduce unnecessary bureaucracy. I am pleased to report that these findings were welcomed and I have been informed that the recommendations made in this respect have already been implemented.

7.5.3. Local Authorities

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.

"Local authorities may only use their powers where they have a clear statutory duty and responsibility to conduct a criminal investigation."

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.

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 141 local authorities notified me they had made use of their powers to acquire

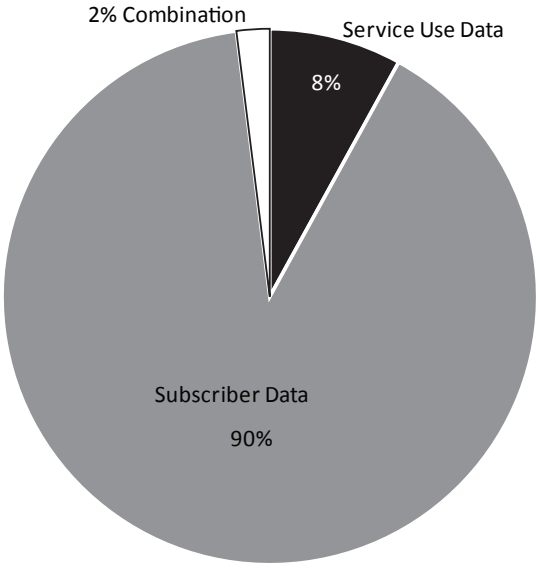
communications data, and between them they made a total of 2,130 requests. This is an increase from the previous year's figures (134 local authorities, 1,809 requests).

> *"58% [of the 141 local authorities that made use of their powers in 2011] made less than 10 requests"*

To put this figure into context, it represents just 0.4% of all communications data requests submitted by public authorities. 79% of the 141 local authorities made less than 20 requests in the reporting period and 58% made less than 10 requests. These percentages are very similar to the previous reporting year.

Figure 10 illustrates that 90% of the 2,130 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 23 of the 141 local authorities acquired service use data under Section 21(4) (b) or a combination of Section 21(4) (c) and (b) data and this accounted for the remaining 10% of requests.

Figure 10 – Local Authority Communications Data Usage



The National Anti-Fraud Network (NAFN) continues to provide a national SPoC facility to those local authorities who wish to use their service. 96 of the local authorities who used their powers this year reported that they are now submitting their requests through NAFN. NAFN was inspected twice during the reporting year due to the increase in the number of local authorities that have signed up to their service. Approximately 70% of the 2,130 requests were managed by the NAFN SPoC Service and this is a significant increase from last year (34%). During the NAFN inspection, my inspectors examined the communications data requests made by 71 individual local authorities. I am pleased to report that NAFN emerged very well from both of their inspections. The Accredited SPoCs at NAFN are providing an excellent service. Overall NAFN is achieving a good level of compliance with the Act and Code of Practice on behalf of its local authority members.

"Approximately 70% of the 2,130 requests were managed by the NAFN SPoC Service.... Overall NAFN is achieving a good level of compliance with the Act and Code of Practice"

During the reporting year 39 inspections were also conducted at local authorities who were not making use of NAFN and for 11 of these local authorities it was their first inspection. Only 18 of the local authorities who reported using their powers in 2011 (but not through NAFN) were not inspected by my team in the said year, but I can report that 6 of these 18 are due to be inspected within the first half of 2012.

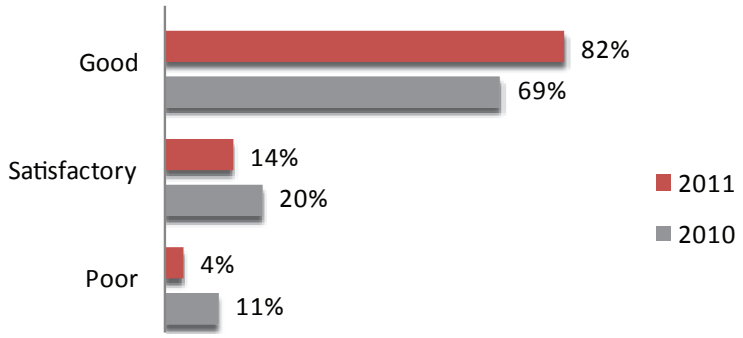
A number of local authorities previously signed up to use the SPoC service provided by a company called SinglePoint. Although quite a number of local authorities signed up, the overall usage of the service was very low. In previous years, my inspectors conducted inspections at a number of the local authorities who reported using SinglePoint to examine the procedures in place. SinglePoint themselves were not inspected as they are not a public authority, however the work they conducted on behalf of the local authorities was fully examined during the individual local authority inspections. Serious failings and weaknesses were identified in the systems and procedures for acquiring communications data at these local authorities and recommendations were made for the issues to be rectified immediately. I was informed in January 2011 that SinglePoint were to cease providing a SPoC service to local authorities.

Figure 11 illustrates that 96% of the local authorities inspected in 2011 achieved a good or satisfactory level of compliance with the Act and Code of Practice and this represents a 7% increase on last year. Only 4% of the local authorities inspected were achieving a poor level of compliance, however if the NAFN results are removed from the overall total, the percentage of poor performing local authorities increases to 10%. These percentages should be treated with caution as the public authorities being inspected are not the same every year.

"96% of the local authorities inspected in 2011 achieved a good or satisfactory level of compliance with the Act and Code of Practice"

Overall four of the local authorities did not emerge well from their inspections and serious failings and weaknesses were found in their systems and processes, some of which will be discussed later in this section. I am pleased to report that these four local authorities are now all using the NAFN SPoC to manage their communications data requests and this should help to resolve the compliance issues.

Figure 11 – Comparison of Council Inspection Results, 2010 vs. 2011



The vast majority of the local authorities that were inspected during the reporting year were completing their applications to a good or satisfactory standard. Even though my inspectors were satisfied that the requests were necessary and proportionate, they concluded that there is still room for a number of the applicants to improve on the quality of their application forms and suitable advice was provided.

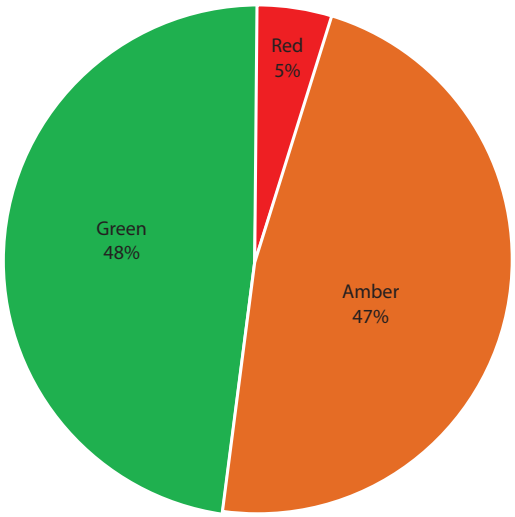
My inspectors found that the DPs were generally discharging their statutory duties responsibly and the vast majority were found to be completing their written considerations to a good standard. However, my inspectors were concerned to find that in five of the local authorities inspected the DPs had not 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 these cases the DPs had mistakenly believed that they did not need to record any considerations. These local authorities have now amended their systems to ensure that they comply in this respect in future. It is important for DPs to comply with this aspect of the Code of Practice to provide evidence that each application has been duly considered.

"In five of the local authorities inspected the DPs had not recorded any written considerations when approving some of the applications and this constitutes non-compliance with... the Code of Practice... These local authorities have now amended their systems to ensure that they comply in this respect in future"

A large number of the local authorities were still not aware that it is the statutory duty of the DP to issue Section 22(4) Notices, despite the fact that I raised this point in last year's report. 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 bearing on the actual justifications for acquiring the data.

I outlined earlier in my report that a traffic light system (red, amber, green) has been adopted for the recommendations that emanate from the inspections. This enables public authorities to prioritise the areas where remedial action is necessary. This year 261 recommendations were made by my inspectors during the local authority inspections and this is an average of 6 recommendations per public authority (if all NAFN users are treated as one). Figure 12 shows the breakdown of recommendations by colour.

Figure 12 – Recommendations from 2011 Local Authority Inspections



Although only 5% of the recommendations represented serious non-compliance with the Act and Code of Practice, these recommendations have highlighted some serious faults in the approval part of the process. It is important however, to recognise that these serious faults only relate to a very small number of the local authorities inspected.

It is also worthy to note that my inspectors identified 77 reportable errors during the 2011 local authority inspections that had not been notified to my office. The causes of the vast majority of these errors, which are related to the DP part of the process are explained below. This is a large number of reportable errors that would otherwise have gone unreported. However it is again important to recognise that the 77 errors all relate to a very small number of the local authorities inspected (9 of the 110 local authorities inspected), and therefore so do the associated compliance issues. I am pleased to report that all of the local authorities have responded very positively to their inspections and I have been provided with assurances that their recommendations have been implemented and that corrective action has been taken where necessary. The findings however do highlight the importance of the inspections.

"these recommendations have highlighted some serious faults in the approval part of the process. It is important however, to recognise that these serious faults only relate to a very small number of the local authorities inspected"

First, my inspectors were extremely concerned to find that in two local authorities the communications data that was acquired had not been approved by a person of sufficient seniority

to act as a DP. In total 52 requests were made by these two local authorities and regrettably this data was therefore not acquired in accordance with the law. It was also shocking to find that the same person had acted as the applicant, SPoC and DP in one of these local authorities. Not only does this represent non-compliance with the Code of Practice, it also means that the requests had a complete lack of scrutiny in the individual local authority as they were effectively self-authorised. The RIPA (Communications Data) Order 2010 (No. 480) makes it very clear that the prescribed officer to act as a DP in a local authority must be a Director, Head of Service, Service Manager or equivalent. I am pleased to report that these two local authorities were quick to put measures in place to ensure that they obtain the appropriate level of authority for any future communications data requests. NAFN has also tightened its DP registration process and the Head of Legal Services / Monitoring Officer from each individual local authority is now required to verify that the person intending to register is of the prescribed rank / level.

"In two local authorities the communications data that was acquired had not been approved by a person of sufficient seniority to act as a DP."

Second, in two instances the DPs in two different local authorities approved the acquisition of traffic data under Section 21(4) (a). Local authorities are not permitted to acquire traffic data but the applications were processed by the SPoCs and approved by the DPs in both of these local authorities. Regrettably in one of these instances the traffic data was disclosed by the CSP and as a result the local authority obtained data to which it was not lawfully entitled. Fortunately in the second instance, the CSP involved refused to comply with the request and did not disclose the traffic data to the Council. The inspectors were satisfied that these two instances were genuine mistakes, but it does emphasise the importance of the SPoC providing a robust guardian and gatekeeper function and the CSPs role in checking the requests they receive.

"In two instances the DPs in two different local authorities approved the acquisition of traffic data under Section 21(4) (a), [which] local authorities are not permitted to acquire"

Third, my inspectors found one instance where a local authority had inappropriately used their powers under Part I, Chapter II of RIPA to acquire communications data in relation to an investigation that did not meet the necessity criteria. The application related to an allegation that a parent living outside of the catchment area of a school provided an address within the catchment area in order to secure a school place. The communications data was requested to provide evidence of residency and to confirm the genuine address. The application stated that the Schools Admissions Department would withdraw the place for the child if the allegation was substantiated, but no criminal offences were specified.

A summary of the case was provided to me by the Council and I was satisfied from this that the conduct undertaken by the Council did not amount to wilful or reckless use of the powers. It is clear that the Council went through a considered thought process, that legal advice was sought prior to submitting the application and that there were ongoing discussions in relation to whether a prosecution was feasible.

Nevertheless, communications data must only be acquired for the purpose of preventing or detecting crime and where there is an intention to gather evidence for use in legal proceedings. It was clear that the predominant purpose for the application was not the prevention and / or detection of crime, but was to enforce the catchment area element of the Council's schools admissions policy, which was not expressed to be supported by a criminal sanction.

It is important to point out that this application was made in 2009, prior to the ruling by the Investigatory Powers Tribunal (IPT) (July 2010) in relation to a similar case involving a surveillance authorisation. The Council became aware of the IPT ruling and shortly afterwards disseminated advice to their staff stating that RIPA powers would not be used for such investigations. It is unfortunate that this application pre-dated the IPT ruling, however my inspector was informed that the communications data acquired did not have an impact on the investigation.

"my inspectors found one instance where a local authority had inappropriately used their powers under Part I, Chapter II of RIPA to acquire communications data in relation to an investigation that did not meet the necessity criteria... The above case, although extremely regrettable, is the first and only instance that my inspectors have found in the 212 individual local authority inspections that have been conducted since 2006. Thousands of applications have been scrutinised since the start of the inspection regime and therefore the evidence that local authorities are frequently using their powers inappropriately is just not there"

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. The above case, although extremely regrettable, is the first and only instance that my inspectors have found in the 212 individual local authority inspections that have been conducted since 2006. Thousands of applications have been scrutinised since the start of the inspection regime and therefore the evidence that local authorities are frequently using their powers inappropriately is just not there.

I still remain unconvinced that the Government's proposal to require all local authorities to obtain the approval of a magistrate before they can use these powers will have much impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data. I do however welcome the Government's proposals to close the loophole through which local authorities are able to use other powers (such as the Social Security and Fraud Act 2001) to acquire communications data. Such other powers are not subject to the same level of scrutiny or oversight.

My inspections have found that a small number of the local authorities have a lack of knowledge and a poor understanding in relation to parts of the process. This is evident from the fact that the local authorities account for 9% of the reportable errors, even though they are making only 0.4% of the overall requests. However in my view, this finding highlights that if local authorities decide to continue to go it alone rather than use the NAFN SPoC service, there is a need for further training to be provided to local authority SPoC staff. My Chief Inspector has recently taken steps to ensure that local authorities are aware of the overall findings from the inspections.

> *"My inspections have found that a small number of local authorities have a lack of knowledge and a poor understanding in relation to parts of the process... This highlights that if local authorities decide to continue to go it alone rather than use the NAFN SPoC service, there is a need for further training to be provided to local authority SPoC staff"*

My inspectors again 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 an example 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. The following example is based on an extract from Sandwell Council's inspection report.

Case Study 14 – Sandwell Council use of Communications Data

Communications data was effectively used in an investigation into the activities of an individual purporting to be a 'faith healer'. The investigation commenced as a result of a complaint received from a husband and wife. They could not conceive a child and had been conned into paying the suspect large sums of money to remove black magic. Subscriber data acquired in relation to a mailing address and telephone numbers identified the suspect and his home address. This allowed a search warrant to be executed and as a result a large amount of evidence was seized, including lists of customers, a mobile phone and pictures. This led to a number of further victims being identified. Unfortunately most of the victims were too scared to make a complaint, however a further three victims did agree to give statements. At Wolverhampton Crown Court the defendant was found guilty of three counts of fraud under the Fraud Act 2006, seven counts of procuring a valuable security by deception contrary to section 20(2) of the Theft Act 1968 and one count of obtaining property by deception contrary to section 15 of the Theft Act 1968. He was sentenced to 18 months imprisonment. Examination of the defendant's bank accounts, accounting records and other non-declared income reveals that in the six years prior to this case, he earned in excess of £4 million from his business as a 'faith healer'. Further proceedings are underway to recover monies illicitly obtained by the offender under the Proceeds of Crime Act 2002.

7.5.4. Other public authorities

There are a number of other public authorities that are registered for the purpose of acquiring communications data. These include the Serious Fraud Office, the Independent Police Complaints Commission, the Gangmasters Licensing Authority and the Office of Fair Trading, to name just a few. The full list of public authorities registered can be found in the RIPA (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.

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 3,443 requests, an increase of 16% on the previous year. However to put this figure in context, it represents just 0.7% of all communications data requests submitted by public authorities. During the course of the reporting year inspections were carried out at 14 of these public authorities. Table 3 lists the public authorities who reported using their powers in 2011.

"During the period covered by this report 23 'other' public authorities notified me that they had made use of their powers to acquire communications data and between them they made 3,443 requests."

Table 3 – All 'other' public authorities who reported using their powers in 2011.

Not Inspected in 2011	Inspected in 2011
• Department for Transport - Rail Accident Investigation Branch. • Department of the Environment (Northern Ireland). • Department for Environment, Food and Rural Affairs. • Environment Agency. • Department for Transport - Marine Accident Investigation Branch. • Maritime & Coastguard Agency. • Child Maintenance & Enforcement Commission. • Information Commissioner's Office. • Office of Communications. • Department of Enterprise, Trade and Investment – (Northern Ireland) Trading Standards Service. • Financial Services Authority (FSA).	• Gambling Commission. • Department of Health – Medicines and Healthcare (Products Regulatory Agency). • National Offender Management Service. • Gangmasters Licensing Authority. • Royal Mail. • Health & Safety Executive. • Office of Fair Trading. • Police Ombudsman for Northern Ireland. • Serious Fraud Office. • NHS Counter Fraud & Security Management Service. • Department of Business, Innovation & Skills. • Independent Police Complaints Commission. • Criminal Cases Review Commission (inspected but did not use their powers in 2011).

Once again the largest user by far was the Financial Services Authority who made 2325 of the 3443 requests (approx 68%). 43% of the 23 public authorities who reported using their powers made less than 20 requests in the reporting period. Figure 13 illustrates that 62% of the 3443

requests were for subscriber data under Section 21(4) (c). 15 of the 23 public authorities acquired service use data under Section 21(4) (b) and these accounted for 8% of the requests. Only 11 of these public authorities acquired traffic data under Section 21(4) (a) and these accounted for 24% of the requests.

Figure 13 – Percentage of Communications Data Requests by Type

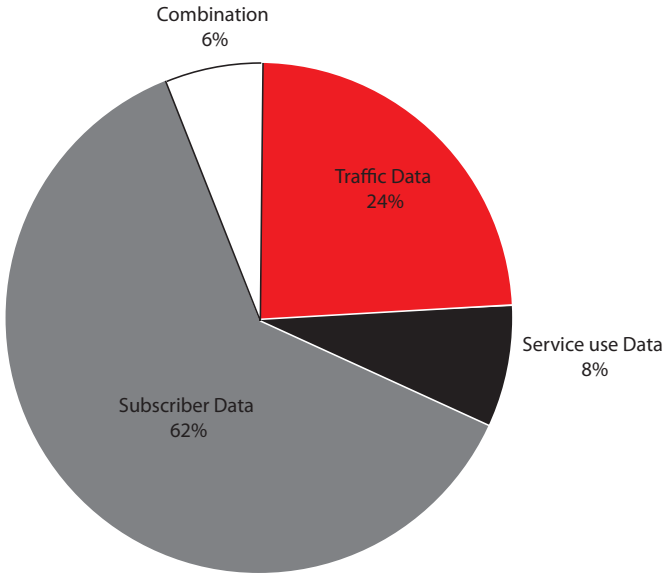
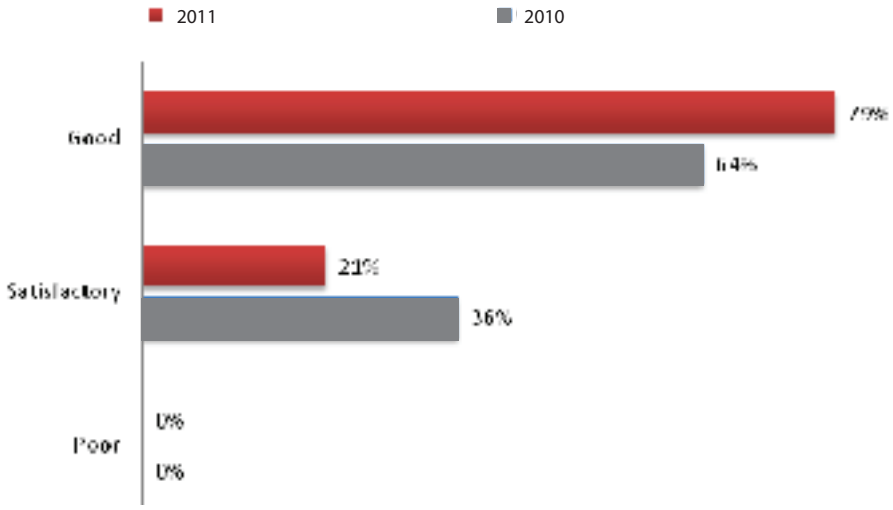


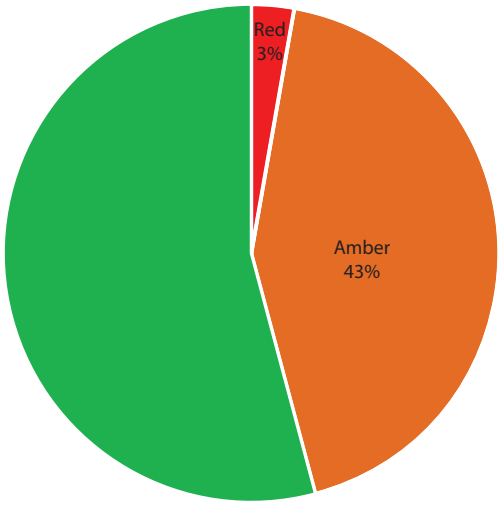
Figure 14 illustrates that 79% of the 'Other' public authorities inspected achieved a good level of compliance with the Act and Code of Practice and this represents a 15% increase on last year. However this percentage should be treated with caution as the public authorities being inspected are not the same every year. 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.

Figure 14 – Comparison of 'Other' Public Authority Inspection Results, 2010 vs. 2011



I outlined earlier in this report that a traffic light system (red, amber, green) has been adopted for the recommendations that emanate from the inspections. This enables public authorities to prioritise the areas where remedial action is necessary. This year 68 recommendations were made by my inspectors during the 'other' public authority inspections and this is an average of 5 recommendations per public authority. Figure 15 shows the breakdown of recommendations by colour.

Figure 15 – Recommendations from 2011 'Other' Public Authority Inspections



The majority of the recommendations were green and these were made to assist the public authorities to improve the efficiency and effectiveness of their processes and reduce unnecessary bureaucracy. The comments I have made in the preceding section of the report in relation to ensuring that Section 22(4) Notices are formally issued by the DPs is equally pertinent to some of these inspections and technical breaches were found in this aspect of the process in 7 of the inspections.

"The majority of the recommendations were green and these were made to assist the public authorities to improve the efficiency and effectiveness of their processes and reduce unnecessary bureaucracy."

The streamlining procedures outlined in Paragraphs 3.30 to 3.32 of the Code of Practice had been misunderstood by one of the public authority's inspected and as a result some of the data that was acquired was not actually approved by a DP. It is important to make the point that these errors had no bearing on the justifications for acquiring the data; nevertheless it is important to ensure that data is always acquired in accordance with the law. A series of recommendations were made to assist the public authority in this respect and I have received an assurance that these have been achieved.

I would like to highlight one investigation undertaken by the Royal Mail where communications data was used effectively. This may provide a better understanding of its importance to the criminal investigations that these types of public authorities undertake.

Case Study 15 – Royal Mail use of Communications Data

Communications data was crucial in progressing an investigation into a series of thefts of special delivery packets, including passports and visas. Royal Mail Investigation Managers suspected that an agency driver who was employed to transport the mail items between Mail Centres (i.e. not on delivery duties) was responsible for the thefts. A wide range of communications data, including incoming and outgoing call data, subscriber checks and location data relating to the suspect and his accomplice was acquired. The data was analysed by the investigator and provided crucial evidence of the identity of the third party involved and the unauthorised stop made in the delivery route where the thefts occurred. The data acquired assisted the arrest and search operations, which uncovered further physical evidence. On 8th March 2012 at Sheffield Crown Court the agency driver was sentenced to 12 months imprisonment, his accomplice received a 6 month custodial sentence suspended for 12 months and 150 hours community service. He was further ordered to pay £4,000 as Royal Mail had paid compensation to customers for the loss of the packets.

The inspections confirmed that the 'other' public authorities that were inspected had restricted the use of their powers to acquire communications data to 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 Part I Chapter II of RIPA were not used for those purposes.

> *"The inspections confirmed that the 'other' public authorities that were inspected had restricted the use of their powers to investigations where they have a clear statutory duty and responsibility to conduct a criminal investigation."*

7.5.5. Training

The National Policing Improvement Agency (NPIA) continues to take responsibility for the training and accreditation of police force and law enforcement agency SPoC staff nationally. 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.

> *"It is very important that all staff who are involved in the acquisition of communications data are well trained."*

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.

As I reported last year, 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 have a good understanding of the procedures. The findings from this year's local authority inspections in particular add further weight to the argument that the national SPoC training should be extended to public authorities in the Section 21(4) (b) and (c) community.

"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."

7.6. Summary of Communications Data Compliance

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 or that I have reported on the small number of occasions that it has not. There is no reason why public authorities cannot make a further disclosure in response to 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.

In the reporting year 99 individual public authorities were inspected by my inspection team and a further 71 local authorities were inspected during the NAFN inspection. 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. Serious compliance issues were identified in a very small number of the public authorities inspected and, although regrettable, I am satisfied these occurred due to genuine misunderstandings, rather than any wilful or reckless failure to comply with the legislation. I have already been provided with assurances that the necessary corrective action has been taken by these public authorities.

I have provided more detailed information in this year's report and I hope that this provides readers with more insight into the rigour of the inspection process and the findings of my inspections.

8. INTERCEPTION OF PRISONERS' COMMUNICATIONS

8.1. General Background

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.

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.

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 Intelligence Unit (IU) at the National Offender Management Service (NOMS) and regular meetings are held to review the outcomes of the inspections.

8.2. Inspection Regime

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.

"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"

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 be asked to 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.

"Communications which are subject to legal privilege are protected"

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.

"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"

The system in place for the recording and monitoring of telephone calls is 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.

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.

"There must be a full audit trail in place in relation to all communications that are intercepted."

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 Advisors Section (PAS) Operational Guidance Documents (OGD3 & 4).

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 read 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 traffic light system (red, amber, green) has been adopted for the recommendations to enable prisons to prioritise the areas where remedial action is necessary. Any red recommendations are of immediate concern as they mainly involve serious breaches and / or non-compliance with Prison Rules and the NSF which could leave the prison vulnerable to challenge. The amber recommendations represent non-compliance to a lesser extent, however remedial action must still be taken in these areas as they could potentially lead to serious breaches. The green recommendations represent good practice or areas where the efficiency and effectiveness of the process could be improved.

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.

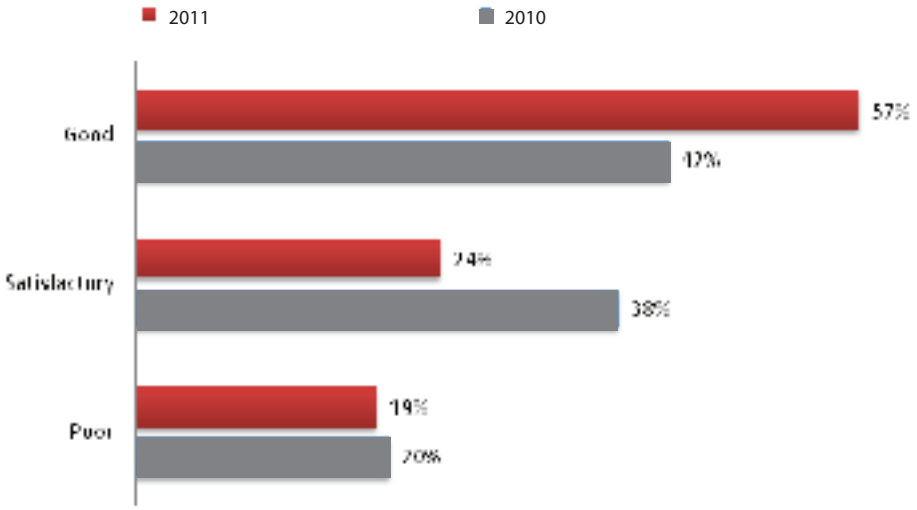
8.3. Review of 2011 Prison Inspections

At the time of writing this report there are 133 prisons in England & Wales subject to inspections and 3 in Northern Ireland. Since the Inspectorate was formed in 2005 two thirds of the prisons have been inspected at least four times. During the period covered by this report my inspectors conducted 80 inspections at 79 prisons, which equates to nearly two thirds of the whole estate. In addition, health checks were also conducted at 2 of the prisons which emerged poorly from their full inspection.

Figure 16 illustrates that 57% of the prisons inspected achieved a good level of compliance with the Act and Code of Practice. This represents a 15% increase on last year's results which is significant. However this percentage should be treated with care as the prisons inspected are not the same every year. These prisons had generally 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 these prisons. In these establishments the managers and staff clearly demonstrated a commitment to achieve the best possible standards.

> *"57% of the prisons inspected achieved a good level of compliance with the Act and Code of Practice. This represents a 15% increase on last year's results which is significant."*

Figure 16 – Comparison of Prison Inspection Results, 2010 vs. 2011



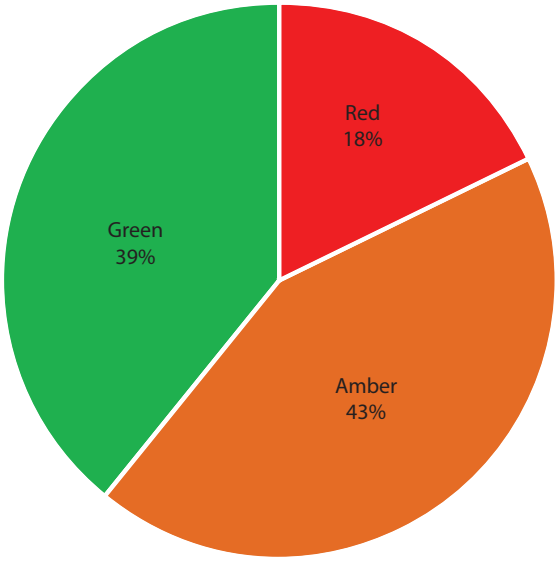
Regrettably serious weaknesses and failings were found in the systems and processes at 15 of the prison establishments. As a result the percentage of poorly performing prisons has remained fairly static. Considering the fact that it was the fifth inspection of six of these establishments, my inspectors expected to see much better standards being achieved. This number is still too high and indicates a failure by managers and staff to ensure that the interception of communications is conducted fully in accordance with the rules. These prisons had mostly failed to implement fully the recommendations from their previous inspections. Two of these prisons have already been subject to health checks and one to a second full inspection. I am pleased to report that these three prisons have worked hard to improve their systems and procedures and they are now achieving a good level of compliance with the rules governing the interception of prisoner's communications. The other prisons have provided an assurance that they will take the necessary remedial action, nevertheless they will also be subject to early re-inspections to check that they have improved their standards.

> *"Regrettably serious weaknesses and failings were found in the systems and processes of 15 of the prison establishments... These prisons had mostly failed to implement fully the recommendations from their previous inspections"*

In last year's report I explained that my prison inspections tend to go in two year cycles due to the number of establishments that require inspecting. Next year I hope to report a reduction in the number of poorly performing prisons.

I outlined earlier in this report that a traffic light system (red, amber, green) has been adopted for the recommendations that emanate from the inspections. This enables prisons to prioritise the areas where remedial action is necessary. This year 547 recommendations were made by my inspectors during the prison inspections and this is an average of 7 recommendations per establishment. Figure 17 shows the breakdown of recommendations by colour.

Figure 17 – Recommendations from 2011 Prison Inspections



The red recommendations fitted into three distinct areas. First, over half of the prisons inspected were found to have failings in either the offence related or intelligence-led Pin-phone monitoring. These failings more often than not result from a lack of equipment and resources to conduct the interception properly, especially when large numbers of prisoners require monitoring.

"These failings [in the monitoring of prisoners telephone calls] more often than not result from a lack of equipment and resources to conduct the interception properly"

Although I am pleased to report that nearly all of the prisons inspected this year had introduced Interception Risk Assessments into the process, approximately a quarter of the prisons were not completing these assessments robustly, which compounds the problem. When properly completed, Interception Risk Assessments provide good evidence to show that the risk factors have been taken into account and they generally lead to a reduction in the number of prisoners requiring monitoring. It is clear that a number of establishments are still struggling with compliance in this respect, even though the monitoring staff are working diligently.

I believe that 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.

"The Prison Service has designed a new interception risk assessment template... hopefully this will assist the prisons to achieve a better level of compliance in this area".

The Prison Service has designed a new Interception Risk Assessment template which has been piloted at a number of prisons and hopefully this will assist the prisons to achieve a better level of compliance in this area. It is also worthy of note that in 17 of the establishments that were not conducting the offence related and / or intelligence-led monitoring of prisoners calls effectively, my inspectors found that random monitoring was still being conducted. It is important for the prisons to ensure that random monitoring takes the lowest priority under the interception strategy. First the monitoring staff must deal with the telephone calls which are made by prisoners who are subject to offence related or intelligence-led monitoring. Recommendations were made to this effect and this should free up some more resources in some of these prisons.

Failure to monitor properly 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. 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 nevertheless the risk is there.

> *"It is important for the prisons to ensure that random monitoring takes the lowest priority under the interception strategy. First the monitoring staff must deal with the telephone calls which are made by prisoners who are subject to offence related or intelligence-led monitoring"*

Second, over a quarter of the prisons inspected were retaining intercept product (generally Pin-phone backup DVDs) for longer than the permitted three month period. This represents a breach of Prison Rule 35D(1). These prisons were instructed to destroy any product that was older than the permitted three month period and monitor the system more closely in future to prevent any recurrence. I have been informed that a planned upgrade to the Pin-phone system will eradicate this issue completely as intercept product will no longer need to be downloaded from the system and will be automatically weeded out once it reaches three months.

> *"Over a quarter of the prisons inspected were retaining intercept product for longer than the permitted three month period... a planned upgrade to the Pin-phone system will eradicate this issue"*

Third, the authorisations in place to conduct the offence related and intelligence-led monitoring were examined by my inspectors and regrettably 9 of the establishments had still 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 be reviewed at least every 3 months, and reviews for intelligence led monitoring must be undertaken within one month. As a result prisoners had continued to be monitored for longer than the permitted period without review. Recommendations were made for these establishments to align their authorisations to the NSF and introduce a robust review process so that monitoring does not continue if an authorisation has expired.

Last year I reported that serious weaknesses and failings were found in relation to the issuing and filing of the Communications Compact in 31 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 20 prisons and these resulted in amber recommendations being made. This was an improvement on the findings from the previous year, however the number of prisons with failings in this area is still too high.

> *"It is important for monitoring logs to be completed to a good standard to show that the monitoring has been conducted, and provide a full audit trail of the interception activity"*

My inspectors also found that there was room to improve the quality of the monitoring logs being maintained by the monitoring staff in over half of the establishments. It is important for monitoring logs to be completed to a good standard to show that the monitoring has been conducted, and provide a full audit trail of the interception activity. The monitoring logs will also assist with the review process and provide the Authorising Officer with the information required to decide whether to continue or cease monitoring.

8.4. Summary

In the reporting year 80 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. Although it was disappointing to find the same number of poorly performing prisons, I am encouraged by the fact that a number of the prisons have clearly improved their level of compliance. A number of prisons now have a dedicated team of well trained staff to conduct the interception of communications and experience shows that this model always achieves better standards.

It is clear that managers and staff are more accustomed to the process and have a better understanding of the systems and procedures that should be in place. There is also evidence from a larger 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.

"A number of prisons now have a dedicated team of well trained staff to conduct the interception of communications and experience shows this model always achieves better standards"

---

9. DISCUSSING MY ROLE

I have taken the opportunity on a number of occasions this year to explain my role by delivering speeches and making formal responses to consultations on intelligence oversight. It is my belief that any speeches I make or interaction I have with international colleagues should focus on the legislation underpinning the lawful interception of communications, how I conduct my oversight role and, to the extent possible, my assessments of compliance at the public authorities I oversee.

9.1. Response to Green Paper

My response to the Government Justice and Security Green paper is reproduced in Annex 1. I conclude in that response that the current arrangements, with judicial and parliamentary oversight of ministerial action, despite being an accident of history, appears to work satisfactorily. Any reform of the system should not place undue additional burdens on the intelligence agencies, and should seek to preserve the accountability of the Secretary of State to Parliament and the electorate.

9.2. Meeting with the Intelligence and Security Committee (ISC)

In March 2011 the current and former Intelligence Services Commissioners, the President of the Investigatory Powers Tribunal and I met with members of the Intelligence and Security Committee (ISC). The ISC was established by the Intelligence Services Act (1994) with a remit to provide parliamentary scrutiny of the expenditure, administration and policies of the intelligence agencies. Our meeting was not a formal evidence session, but we did have a useful exchange of views about our roles and our assessments of compliance at public authorities, their relationships with the agencies, levels of access to relevant intelligence, sampling of cases for review, and error reporting. The session concluded with a substantive discussion on proposals for intelligence oversight reform being outlined within the Justice and Security Green Paper.

9.3. Data Protection Forum

I accepted an invitation in December 2011 to speak to the Data Protection Forum on my role as commissioner. The Data Protection Forum represents a group of industry professionals involved in securing the protection of personal data held by government departments, private companies and other entities. I spoke to the group about differences between communications data and lawful intercept, my role as defined by RIPA, the role of my inspectors and the wider office, the error reporting system in relation to lawful intercept and communications data, my assessment of compliance by those whom I oversee and finally my interaction with the Information Commissioner. I was grateful for the opportunity to share my views.

9.4. International delegations

I was pleased this year to receive international colleagues from both South Africa and Canada in order to share views on differing models of intelligence oversight in our respective countries.

9.4.1. Ambassador Faith Radebe, Inspector-General of Intelligence, Republic of South Africa

I met with a delegation from South Africa led by Ambassador Faith Radebe in 2011. Ambassador Radebe, a lawyer by profession and former High Commissioner to the Caribbean, took up the post of inspector General in April 2010. There were particular issues of shared interest that I was able to discuss with the Inspector-General, which included our respective national interception frameworks, our respective mandates, legislation covering the oversight of intelligence services, the balance of parliamentary and independent oversight, accountability structures, access to information, tasking and future collaborations.

9.4.2. Canadian Security Intelligence Review Committee (SIRC)

The President and Vice-President of the IPT and I hosted members of the Canadian Security Intelligence Review Committee (SIRC) in November 2011. SIRC is an Independent external review body which reports to the Canadian Parliament on the performance of the Canadian Security and Intelligence Service (CSIS). We were able to discuss how in many ways SIRC played an analogous role to the IPT, the commissioners and, in terms of its focus on conducting thematic reviews, the ISC. The meeting focussed on the mechanics of my oversight function, challenges around protecting sensitive information, how I assured myself of compliance at those agencies I oversee, and my levels of interaction with other intelligence and security bodies. I was happy to share my views on these matters.

10 INVESTIGATORY POWERS TRIBUNAL

Section 57 (3) of RIPA requires me to give all such assistance to the Tribunal as it may require in relation to investigations and other specified matters. My assistance was not sought by the Tribunal during 2011.

The IPT published a report in 2011 which gives information about its members, policies and procedures. It also provides statistics on the kinds of claims it receives, and other matters. The report is available on the IPT website www.ipt-uk.com.

11 CONCLUSION

The use of lawful interception and communications data affords significant advantages to law enforcement bodies, intelligence agencies and other public authorities when investigating the variety of threats faced by the UK. However, due to the potential intrusion into an individual's private life that interception and the acquisition of communications data may involve, it remains crucial to have effective oversight.

During a period of proposed reform to intelligence oversight, a number of key principles that define the use and oversight of interception techniques and communications data in the UK should be preserved.

First, the process by which oversight is conducted should be as transparent as possible. So in this year's report I have disclosed further details of how I, and my inspectors on my behalf, conduct our inspection visits, whom we meet and the matters discussed. I have also disclosed the total number of interception warrants signed by Secretaries of State and Scottish Ministers. This fulfils the objective of enabling readers to discern the total pool of warrants from which I select my samples for review during inspection visits without revealing information that may be detrimental to national security. When issues of compliance arise these have also been set out in this report.

There are, however, items the disclosure of which in my public report may be detrimental to national security. Any reasonable member of the public would agree that names of targets and intelligence techniques cannot be disclosed because disclosure could harm national security. I can, however, disclose some matters to senior intelligence officials and Ministers engaged in interception. So this year I have, with the agreement of the Prime Minister and those whom I oversee, produced a confidential supplement to my open report containing further details of those policy and legal matters on which I have been consulted by the public authorities I oversee. It is my intention to distribute this supplement to a select group of senior intelligence officials and Ministers so they can have a better understanding of what is being overseen, how it is being overseen, and the impact of such oversight.

Second, I have observed that, as has always been the case, the greatest scrutiny occurs within public authorities themselves. For example, in relation to lawful interception, an authorisation must cross the desks of a number of officials, sometimes including legal advisers, and it will be scrutinised with care several times before it reaches the Secretary of State or Scottish Minister. Similar safeguards exist in relation to the acquisition of communications data; a request must be vetted and quality assured by an accredited SPoC before being considered by a Designated Person of an appropriate rank who sits outside the investigation for which the communications data is being requested. I have observed that ministers, officials, law enforcement officers and members of CSPs undertake this internal scrutiny with dedication and integrity.

Third, it should be recognised that my assessment of compliance at those departments and agencies I oversee is based on a number of sources. It is informed not only by the inspection of interception warrants, but also interaction with a cross-section of officials and Secretaries of State or Scottish Ministers involved in lawful interception throughout the year, in addition to feedback from my inspectors in relation to their communications data and prison inspections and the reporting of errors.

Error reporting represents a significant component of my oversight function. The likelihood of my selecting a faulty warrant as part of my inspection visits, is reduced by the fact that the agencies themselves report errors to me when they are discovered, in addition to making information about these errors available for review during inspection visits. Due to the greater number of communications data requests in the UK, errors are both reported by public authorities and as set out in this report, discovered by my inspectors during their inspection visits. I am confident that errors are generally reported on time, in full and that steps are taken to reduce the likelihood of such errors being repeated.

I recognise that there are proposals to update interception legislation and reform intelligence oversight. It is my belief that lawful interception and the use of communications data represent significant, cost-effective tools in the fight against the growing number and variety of threats faced by the citizens of the UK. There is a substantial structure which has been developed to ensure that the use of interception and communications data is properly authorised as an investigative technique. I believe it is right to update the legislative framework so far as is necessary to ensure that investigative techniques keep pace with new forms of communications usage by those who wish to do harm to the UK. However, I also believe that any increase in powers should be properly overseen within a balanced system.

Balance is a key component of the current system of intelligence oversight in the UK. It should be preserved in any future reforms. Our system of oversight, which involves judicial, parliamentary and internal scrutiny, despite being to some extent an accident of history, appears to work effectively. The public authorities seem to welcome my oversight, within the context of a mutually beneficial, constructive relationship based on trust and openness. Any reform of the system should seek to preserve this balance and not place any additional burden on those public authorities who seek to protect the UK.

Finally, I would like to restate, as in previous years, that my work would not be possible without the secretariat and inspectors who work with me. I also extend my thanks to Sir Mark Waller, the Intelligence Services Commissioner and members of the Investigatory Powers Tribunal. They have all done excellent work and I continue to be very grateful.

12 ANNEX A

INTERCEPTION OF COMMUNICATION COMMISSIONER'S RESPONSE TO THE JUSTICE AND SECURITY GREEN PAPER

1. Introduction

Chapter 1 sets the scene and makes the case for change. Chapter 2 makes proposals for dealing with sensitive material in civil proceedings. The proposals involve the conduct of civil proceedings and touch upon the role of the Investigatory Powers Tribunal. As to the conduct of civil proceedings it seems to me that the responses would be most helpful if they come from serving Judges (possibly via the Office of the LCJ), and so far as the IPT is concerned I understand that it will respond in relation to Chapter 2.

Chapter 3 begins by dealing with Ministerial responsibility and Parliamentary oversight (the Intelligence and Security Committee: ISC). This is not an area that calls for comments from a serving commissioner, so I concentrate on the paragraphs beginning with 3.39. They begin with a proposal to expand the statutory role of the Intelligence Services Commissioner (para 3.43) and I leave that to him.

The Paper then outlines the possible role of an Inspector-General before posing two questions.

Q1: What changes to the commissioners' existing remit can best enhance the valuable role they play in intelligence oversight and ensure their role will continue to be effective for the future? How can their role be made more public facing? Are more far-reaching proposals preferable, for instance through the creation of an Inspector-General?

The auditing role of the Interceptions Commissioner is clearly set out in the statute. It has clear boundaries, and seems to work well in practice. I see no compelling reason to change the nature of the role or the boundaries. I accept that the work could be undertaken as part of the role of an Inspector-General, but that might not be so patently independent, nor would it be any cheaper. Furthermore the role would not be, nor could it be, any more public facing than it is already because of the nature of the material being examined. The procedures used by the commissioner and his inspectors are clearly set out in the Annual Reports, and from time to time in lectures. Information is provided so far as it can be provided but, for good and compelling reasons, the whole picture cannot be disclosed.

Q2: Are more far-reaching intelligence oversight reform proposals preferable, for instance through the creation of an Inspector-General?

The IG model clearly works well in other jurisdictions, but it does have its drawbacks- it creates a fresh quango. The incumbent can easily be accused of being too close to Government, or too keen to find fault with the security services. Our arrangements are, to some extent, an accident of history, but they do achieve a neat balance between political accountability and independent judicial scrutiny. In response to the question it is appropriate to ask what benefits would be

conferred by the creation of an IG, with an office and supporting staff, which we do not already enjoy, or cannot obtain by some relatively minor adjustments to our present arrangements. The only benefit which comes to mind is that an IG could choose to review the operational decisions of the services. But such a review can only really be justified if something seems to have gone badly wrong, and our existing arrangements allow for that. Otherwise operational decisions must be in the unfettered control of the Director of the relevant service, who is answerable to the Minister, and I do not see what is to be gained by subjecting the Director to the oversight of an IG.

The Green Paper then deals with the need to ensure that there is a balanced system, pointing out that, for instance, some powers which might be given to the ISC could not be given if there was an IG.

Two subsequent questions are then posed:

Q3: What combination of existing or reformed arrangements can best ensure credible, effective and flexible independent oversight of the activities of the intelligence community in order to meet the security challenges of today and the future?

So far as lawful interception is concerned I am content with the combination of arrangements which at present exists. I have complete access to warrantry materials, and to records in relation to data which has been obtained, and my inspectors and I are completely independent. So we have the full powers and professional integrity of any auditor, but we are not the only safeguard against abuse. An important additional safeguard is that every application for a warrant or for data is scrutinised at a number of levels before it is approved, so the possibility of successful deliberate abuse is very small indeed, if statutory channels are being used. But it is also important to emphasize the roles of the Secretary of State and the ISC. Without impinging on my role they have separate roles and provide political accountability, which is particularly important in an area that cannot be opened to public scrutiny.

Q4. With the aim of achieving the right balance in the intelligence oversight system overall, should greater emphasis be placed on reforming parliamentary oversight or independent oversight?

For the reasons I have given I see no reason to press for any reform to the role of the Interception Commissioner in providing oversight in his particular territory, the boundaries of which are clearly defined. It is also obvious that the commissioner cannot be accountable to the Secretary of State, whose actions he reviews, or to the ISC. I do not, however, consider it appropriate for a serving commissioner to offer any comments in relation to reform of parliamentary oversight.

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

HO_01939_G