# 2012 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 18th July 2013

Laid before the Scottish Parliament by the Scottish Ministers July 2013

HC 571
SG/2013/131

£16.00

# 2012 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 18th July 2013

Laid before the Scottish Parliament by
the Scottish Ministers July 2013

HC 571
SG/2013/131

£16.00

**Any enquiries regarding this publication should be sent to ch2.inspectorate@iocco.gsi.gov.uk.**

**You can download this publication from www.iocco-uk.info.**

**ISBN: 9780102986594**

**Printed in the UK by The Stationery Office Limited**

**on behalf of the Controller of Her Majesty's Stationery Office**

**ID 2574865 07/13**

**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 Kennedy served as the Interception of Communications 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 role annually since 2006, I move now to my final report, covering the period between 1st January and 31st December 2012. I stood down as Interception of Communications Commissioner at the end of this period and am not in a position to deal with events after that period.

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 communications data acquisition remain crucial techniques for the UK's intelligence agencies, law enforcement bodies and wider 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.

The report for 2011 was well received, and I report in the same level of depth this year. I have repeated information which I believe is necessary for readers to understand my oversight of lawful interception, communications data and interception of prisoners' communications without reference to previous reports.

**The Rt Hon Sir Paul Kennedy**
Interception of Communications Commissioner
(2006-2012)

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

RIPA and the way in which it defines 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.

It may be helpful to restate here the difference between lawful interception and the acquisition of communications data. Although both fall under my remit to oversee, they are authorised at different levels and used to different extents.

The power to acquire the 'content' of a communication, be it an email, telephone call or text message, is provided under Part I Chapter 1 of RIPA. In order to intercept a communication lawfully a warrant, signed by a Secretary of State, is required.

Part I Chapter 2 of RIPA provides the power to acquire communications data. This represents the 'who', 'when' and 'where' of a communications event. In order to acquire communications data, a designated person of an appropriate grade within a public authority with the requisite powers under RIPA must approve the request.

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 these two areas.

Figure 1 outlines the relevant sections of the statute governing the use of RIPA powers.

**Figure 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 communication (i.e. Phone call, email, text message, letter) | In the interests of national security.<br>Prevention or detection of serious crime.<br>Safeguarding the economic well-being of the UK. | Intelligence Services:<br>– Government Communications Headquarters (GCHQ)<br>– Security Service (MI5)<br>– Secret Intelligence Service (SIS)<br>Serious Organised Crime Agency (SOCA).<br>Scottish Crime and Drugs Enforcement Agency (SCDEA).<br>Metropolitan Police (Met).<br>Police Service for Northern Ireland (PSNI).<br>Scottish Police forces.<br>Her Majesty's Revenue and Customs (HMRC).<br>Ministry of Defence (MoD) 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 Interception 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 2 | 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.<br><br>Prevention and detection of crime or prevention of disorder.<br><br>Safeguarding the economic well-being of the UK.<br><br>In the interests of public safety.<br><br>For the purpose of protecting public health.<br><br>For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.<br><br>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.<br><br>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.<br><br>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 Interception of Communications Commissioner through a team of inspectors. |
| Pt. III | The investigation of electronic data protected by encryption. | Interests of national security.<br><br>Prevention and detection of crime.<br><br>Interests of economic well-being of United Kingdom; or<br><br>For the purpose of securing the effective exercise or proper performance by any public authority of any identified statutory power or statutory duty. | Any public authority. | Authorisation is most frequently by a judge. | Oversight is conducted by the Interception of Communication, Intelligence Services and Surveillance Commissioners', except when authorised by a judge. |

# 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 upon 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 interception. What is meant by lawful interception 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 2 of Part I.** This refers to the acquisition and use of communications data. What is meant by communications data is more fully explained in Section 7.
- **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. 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.
- **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 under Chapter I, and, the duties imposed by section 55 (so far as applicable) to information obtained under Part III.

It is also my function under RIPA to give the Investigatory Powers Tribunal, set up under Section 65 of RIPA, 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 2012, but when sought it has willingly been given.

In addition my predecessor agreed to undertake a non-statutory oversight regime in relation to the interception of prisoners' communications and my team has continued to do that work.

My remit is therefore quite extensive, but it is circumscribed. I do not have blanket oversight of the intelligence agencies, wider public authorities or prisons, and I am not authorised to oversee all of their activities. In essence my inspectors and I act as auditors in relation to RIPA. We look at the information on which decisions were made, consider whether the decisions taken were necessary and proportionate, and, examine how the material was acquired, handled and used. Also in many cases we are able to see what was achieved as a result.

# 5. SUCCESSES

I continue to be impressed, as in previous years, with the role that lawful interception and communications data acquisition plays in the operational successes of intelligence agencies, law enforcement agencies and other relevant public authorities in the UK. Interception and communications data remain powerful techniques in the investigation of many kinds of crime and threats to national security. Many of the largest drug-trafficking, excise 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/or communications data.

The following case summaries are just a sample of a large number of operations that have been examined during the 2012 inspections where lawful interception and/or communications data have played a role in a successful outcome. I have, as in previous years, not provided detailed examples of operations from the intelligence agencies in order not to prejudice national security.

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

### Case Study 1 – SOCA - Use of Lawful Interception

SOCA used intercept intelligence to good effect when investigating the Class A drug trafficking activities of a UK based Organised Crime Group (OCG) in 2011 and 2012. A number of individuals involved in the collection, storage and distribution of Class A drugs were identified. SOCA was able to arrest several individuals and seize a large quantity of drugs. In spite of this, the principal member of the OCG continued to coordinate the supply and distribution of controlled drugs.

Intercept intelligence assisted SOCA to seize a firearm and a large amount of ammunition that was going to be used in the shooting of a rival OCG member to settle an ongoing drug dispute, and to identify other members of the OCG that were involved in the laundering of cash derived from the sale of Class A drugs.

Overall in excess of 30 people associated to these OCGs were arrested for offences of supply and distribution of controlled drugs, money laundering and possession of firearms. SOCA were enabled to seize in excess of 100kgs of Class A and B drugs, a firearm and over £175,000 in cash. During the course of the investigation, actionable intelligence was disseminated by SOCA to police forces and international law enforcement partners, providing a valuable contribution to law enforcement efforts in the UK and abroad. Of the individuals subject to interception, approximately half were convicted for drug related offences, receiving prison sentences totalling over 100 years.

### Case Study 2 – Use of Communications Data - Environment Agency

Communications data was used to good effect to develop intelligence in relation to Operation Brynce, an investigation into the activities at a major illegal waste site in Cornwall. Several thousand tonnes of waste were dumped at Rocks Farm in Bugle between 2003 and 2011 after it was turned into an illegal waste transfer station and landfill. Waste was burnt, sorted, sold and recycled from the site, despite the fact that there was no planning permission from Restormel Borough Council or the necessary permits from the Environment Agency.

Subscriber / account data was acquired on key telephone numbers and this established that the illegal operation was a family concern. The communications data that was acquired also led to the identification of a number of key suspects who were working behind the scenes arranging for the collection and disposal of waste.

The Environment Agency estimated that more than 4,500 cubic metres of material had been land filled at the site. The family also let out 51 caravans at the site which they did not have a permit to operate. The site was not connected to the mains sewer and had its own septic tank system. The Environment Agency checked the system, which revealed it was inadequate. The family's operation undercut legitimate businesses and legitimate waste sites. The sewage seeping from the tank was a health issue and posed a risk to the water course and ground water.

At Truro Crown Court, 8 defendants pleaded guilty to criminal offences under the Environmental Protection Act 1990 or the Water Resources Act. The defendants will be sentenced later in 2013 and are subject to a confiscation hearing.

## Case Study 3 – Use of Communications Data - West Midlands Police

Communications data was used effectively in this investigation where a female offender posed as an undercover police officer when committing various fraud offences. In this guise she convinced an elderly lady to work with her to investigate how shops and banks deal with customers. She persuaded the victim to purchase high value items, such as iphones, for which she would purportedly be reimbursed at a later stage. At the time the police identified the offence, the victim had been defrauded of £11,000 and had unwittingly facilitated the purchase of between £2-3,000 worth of high value goods. The victim was also on the point of selling her home for £138,000, which was about to be paid to the fraudster.

At the early stages of the investigation attempts were made to identify the fraudster. Subscriber and service use data was acquired on the fraudster's contact numbers which had been provided to the victim and on the phones that the victim had purchased. Unfortunately this did not further the investigation.

However, the police were aware of a number of distraction burglaries and intelligence suggested a known female criminal was responsible. The victim was unable to pick out the suspect at an identity parade and, although some CCTV footage was available, it did not provide sufficient evidence to fully identify the suspect.

At this stage a communications data strategy was devised and concentrated on a mobile phone for the suspect that was identified through overt police systems. Service use data acquired on this phone showed contact with the elderly lady and a number of the victims of the distraction burglaries. Traffic data was acquired and the analysis of this data demonstrated that the suspect had been in the vicinity of the offences. The communications data directly led to the arrest of the suspect who was charged with 10 fraud offences. The suspect and an accomplice were found guilty and sentenced to 8½ years and 2 years imprisonment respectively.

# 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 intelligence and law enforcement agencies in the interests of national security, for the prevention and/or detection of serious crime, and to safeguard the economic well-being of the UK (where this is directly related to national security).

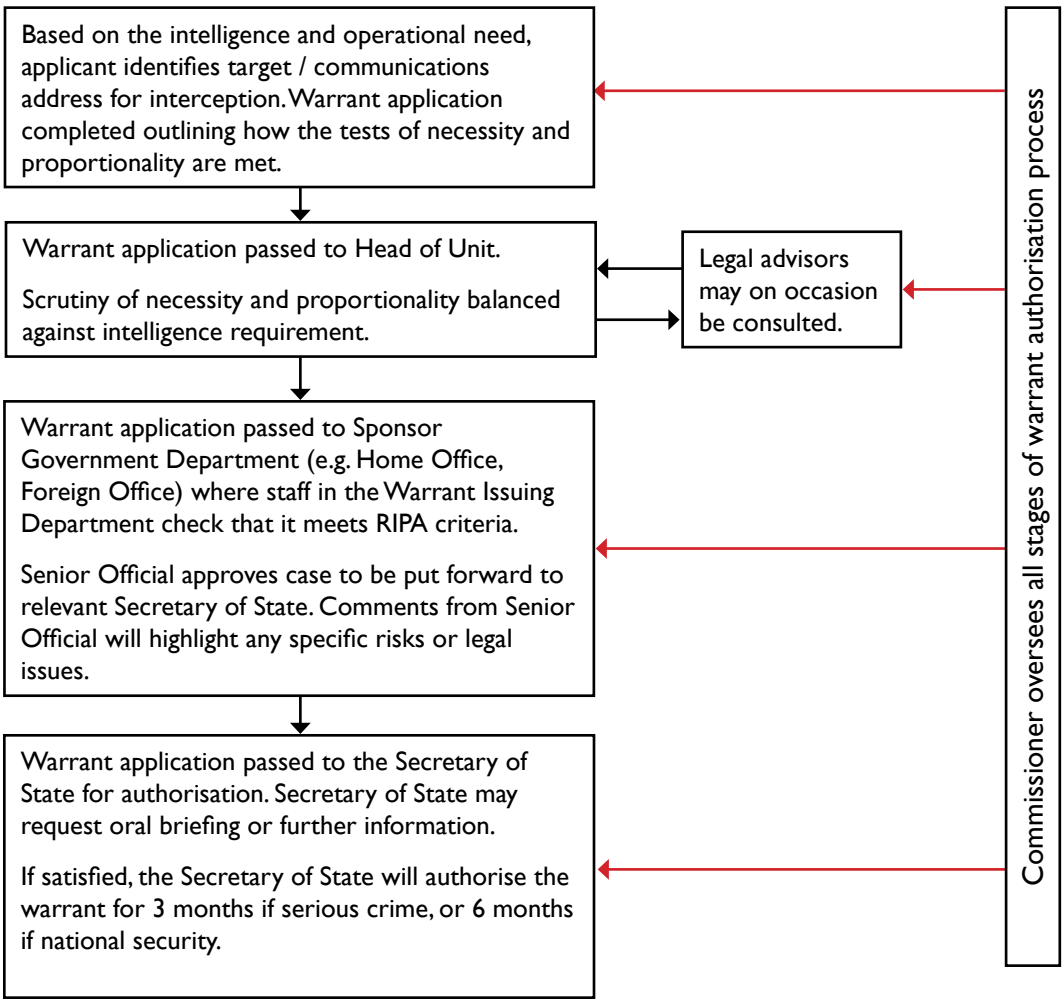
Section 2 of RIPA defines the meaning and location of interception:

> *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."*
>
> *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 interception, RIPA requires that interception of communications can only be authorised by a warrant signed by a Secretary of State or Scottish Minister[1].

1 Scottish Ministers are the appropriate authority in relation to serious crime in Scotland. In this report the wording 'Secretary of State' should also be taken to mean 'Scottish Minister.'

## Figure 2 - The Warrantry Authorisation Process




As detailed in Figure 2, the role of the Secretaries of State 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 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 my inspection visits in relation to lawful interception under Part I, Chapter 1 of RIPA. This section, to the extent allowed without revealing sensitive details, provides further information on how such inspection visits are conducted.

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 the Warrant Issuing Departments of State from which warrants are obtained.

When the inspection takes place I examine the warrants and supporting paperwork presented to the Secretary of State. I need to be satisfied that at the time when the warrant was obtained, the Secretary of State was entitled to conclude that it was necessary and proportionate to grant it for one of the statutory purposes, despite the intrusion 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. I seek to satisfy myself that the relevant safeguards within the Code of Practice have been adhered to. I discuss the rationale behind the warrants with the agency staff and the benefit derived from the warrant. I am also able to view the product of any interception that may have been authorised. As last year, I have set out in Figure 3 the stages and purposes of a typical inspection visit.

## Figure 3 – An Inspection Visit

| Stage | Description | Purpose |
|---|---|---|
| Selection Stage | Warrant Issuing Department (WID) or Law Enforcement Agency (LEA) provide list of extant, expired and modifications to authorisations since last inspection visit.<br><br>Agencies also commonly refer Commissioner to specific cases of interest concerning either errors or legal issues.<br><br>Commissioner randomly selects a number of warrants and authorisations for further scrutiny on inspection day. | Checks are made by WID and Secretariat to ensure all authorisations are submitted.<br><br>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.<br><br>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.<br><br>Where necessary, oral briefings provided by case officers to detail intelligence case behind the submissions and answer any questions the Commissioner has. | 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.<br><br>Commissioner seeks to reassure himself that throughout the authorisation process the principles of necessity, proportionality and other safeguards have been applied.<br><br>Specific focus on ensuring renewals are submitted in good time and that urgent oral applications really are urgent. |
| Follow-up stage | Meetings with relevant Secretary of State. Discussions with Senior Officials at Department of State through whom submissions go before reaching Secretary of State.<br><br>Report of Inspections within Annual Report. Informal consultation between the Intercepting Agencies and Commissioner on challenging legal or policy issues. | Ensure getting best value from Commissioner's expertise.<br><br>Characteristic of an effective relationship between the Commissioner and the Intercepting Agencies. |

Throughout my 2012 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 Warrant Issuing Department of State before reaching the relevant Secretary of State.

## 6.3 Lawful Interception Warrants

I am once again able to report a single figure comprising the total number of lawful interception warrants signed by the Secretaries of State.

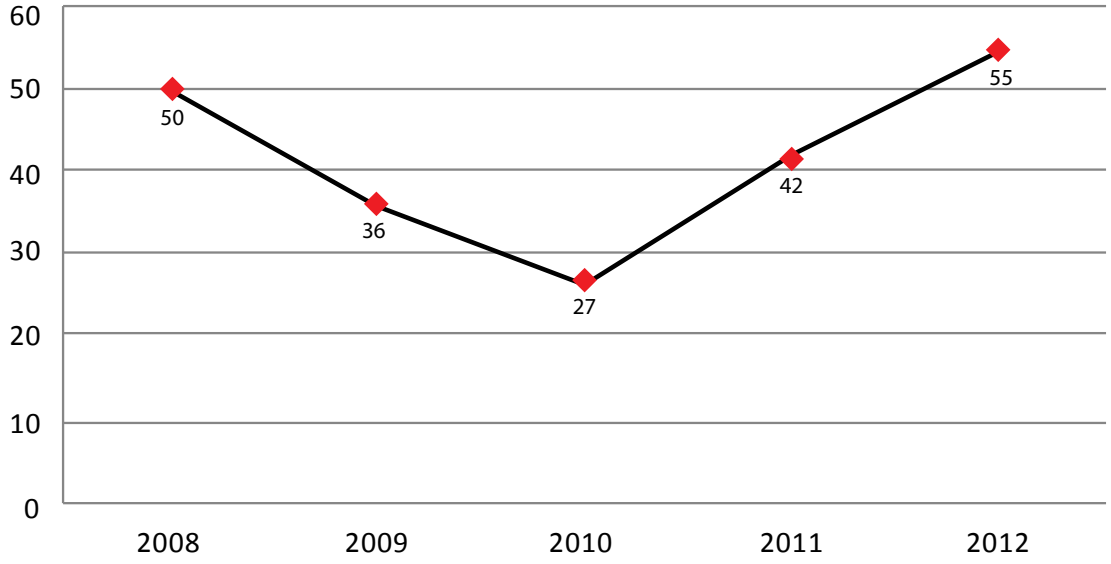
This figure fulfils the objective of enabling readers to discern the total pool of warrants from which I select my samples for review during inspection visits whilst not disclosing sensitive information, for example on the extent of coverage of any specific target that may be detrimental to national security.

The total number of lawful intercept warrants issued in 2012 under Part I Chapter I of RIPA was 3372. This represents a 16% increase on the number of lawful intercept warrants issued in 2011. I do not set out the number of warrants that are extant at the end of the year because for present purposes that is unnecessary, and because to do so could provide hostile agencies with information as to the interception capabilities of the UK which could be of value to them.

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. 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 significant.

## 6.4 Interception Errors

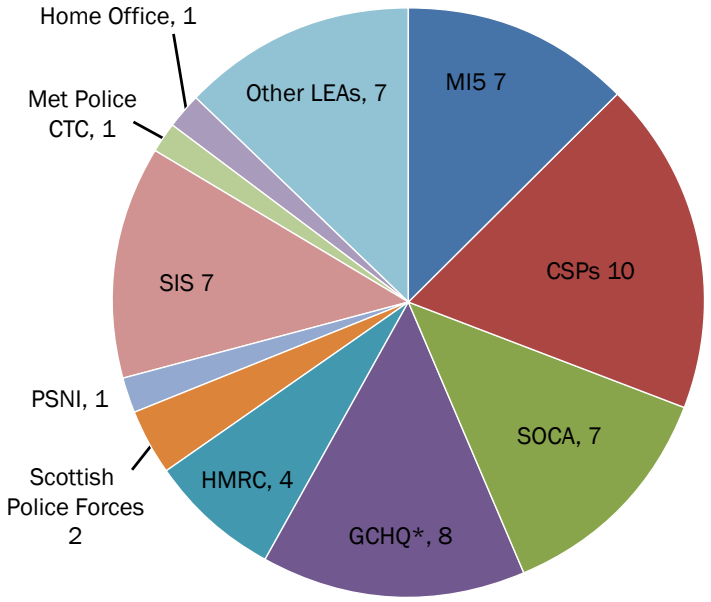
**Figure 4 – Total Number of Intercept Errors over the previous 5 years**




During the reporting year, 55 errors / breaches were reported to my office by public authorities. This represents a 30% increase on the 42 errors reported in 2011. However, 2 points are worthy of note. First, the number of warrants did increase by 16% in 2012. Second, for the first time, the error figures have also included breaches under Section 1(5) of RIPA that were caused by law enforcement agencies not having the necessary authority in place to acquire stored communications (such as text messages, voicemails and emails). There were 7 such breaches this year (13% of all errors) and it is important to note that these errors were not made by the interception agencies in relation to lawful interception warrants.

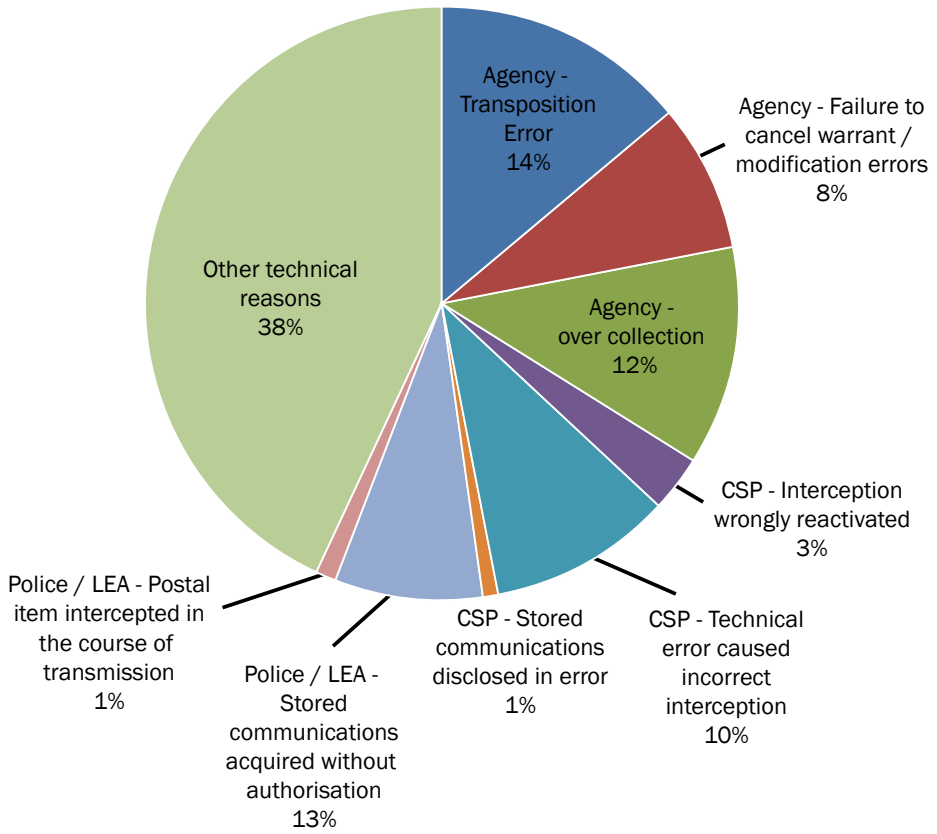
Figure 5 illustrates the breakdown of errors by responsible party and Figure 6 illustrates the breakdown of errors by cause.

## Figure 5 – 2012 Breakdown of the number of Intercept Errors by Interception Agency / Law Enforcement Agency / CSP




*This year's report includes 3 errors that actually occurred in 2011 as they were not discovered and/or fully investigated until after the cut off period in 2012.

## Figure 6 – 2012 Breakdown of errors by cause



The comprehensive error reports I have received during the year, supported when necessary by thorough explanations during inspections, allows me to conclude none of the errors reported were malicious or deliberate. Each error involved some kind of human error or system related technical problem. In a large number of the 55 error cases, no intercept product was actually obtained and therefore there was no unjustified or unnecessary intrusion. In the smaller number of cases where intercept product was wrongly obtained, I have been assured that any such product has been destroyed. In all cases the reporting agencies have taken steps to reduce the risk of recurrence, whether this is achieved by further training or guidance or technical fixes to systems.

Although I have explained that the increase in the number of errors is mainly down to two factors, any increase in errors is extremely 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.

## 6.5 Inspection Results

This section deals with the outcomes of the inspections that I undertook in 2012 in relation to lawful interception under Part I Chapter I 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.

There are, however, a small number of 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. This year I have again produced for the consideration of the Prime Minister, a confidential annex to this open report containing further details of the policy and legal matters on which I have been consulted by the agencies I oversee. It is my intention, subject to his agreement, to distribute this annex to a select group of senior intelligence officials and Secretaries of State engaged in interception.

### 6.5.1 GCHQ

My formal inspection visits to GCHQ took place in April and October 2012. I selected a number of warrants of varied types to review. 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.

In addition, GCHQ legal advisers have taken the opportunity to discuss emerging capabilities with me outside of the inspection visits. We also discussed the planning and preparation for the 2012 London Olympic and Paralympic Games.

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

### 6.5.2 Secret Intelligence Service (SIS)

My formal inspection visits to SIS took place in April and October 2012. Prior to my inspection I selected a number of warrants of varied types to review.

During my inspection I received presentations in relation to specific interception warrants and, when necessary, was able to discuss the rationale behind the warrants with the officers concerned. 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.

We also discussed the technical errors reported to my office and I was satisfied with the measures put in place to prevent recurrence.

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

### 6.5.3 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 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 during these visits.

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.

My formal inspection visits were held in May and October 2012. 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.

### 6.5.4 Security Service (MI5)

My formal inspection visits to MI5 took place in May and October 2012. Prior to the inspection I selected a number of warrants of varied types to review. During my formal inspection visits to MI5, I met the Director General and held meetings with Deputy Director General alongside the heads of various divisions focussed on counter-terrorism, counter-proliferation and counter-intelligence. We also discussed the planning and preparation for the 2012 London Olympic and Paralympic Games.

I received presentations in relation to specific interception warrants and, when necessary, was able to discuss the rationale behind the warrants with the officers concerned and legal advisers.

I was again impressed by the attitude and expertise of the staff I met who are involved in the interception of communications and I am satisfied that they act with the highest levels of integrity.

### 6.5.5 SOCA

My formal inspection visits to SOCA took place in April and October 2012. SOCA has a wide remit and acts as the intercepting agency for the police forces and other law enforcement agencies in England and Wales. I selected a number of warrants in relation to serious criminality, including warrants relating to drugs supply, firearms supply and use, armed robberies, money laundering, kidnaps / threats to life and corruption.

I received presentations in relation to specific interception warrants from the case officers and I was able to discuss with them both the rationale behind the warrants and the results that had been achieved. I was impressed with the diligence and commitment of the staff I met.

During these inspections I discussed a sensitive matter in relation to a breach of the Section 15 safeguards. I was satisfied with the investigation that SOCA were conducting into this breach. I also discussed the renewal process with SOCA and concluded that the current process is relatively unsatisfactory, largely due to the fact that they have to prepare the renewals so far in advance that they have not had the opportunity to gather intelligence over anywhere near the full three month period that was authorised by the Secretary of State. I discussed this issue at my meeting with the Home Secretary referred to later in this section.

### 6.5.6 HMRC

My formal inspection visits to HMRC took place in April and October 2012. I selected a number of warrants in relation to various types of serious criminality including, tobacco smuggling, alcohol smuggling, VAT fraud and money laundering. When necessary I was able to discuss the rationale behind the warrants with the warrantry staff.

I was satisfied with the information provided to me at HMRC and with the professionalism and knowledge of the staff involved in the interception of communications. We also had a useful discussion in relation to the current and future challenges of internet based communications.

### 6.5.7 Metropolitan Police Service (MET) Counter Terrorism Command (CTC)

My formal inspection visits to the MET CTC took place in April and November 2012. The Met CTC operates against the threat of terrorism at a local, national, and international level. It has the national lead for domestic extremism and also deals with sensitive national security investigations.

I selected a number of warrants to review during the inspection relating to domestic extremism, corruption, the supply of firearms and/or drugs and other serious criminality on the periphery of MI5 national security investigations. I was able to discuss the rationale of the warrants with the warrantry staff and was particularly impressed with the quality of the documentation. We

discussed the fact that the MET CTC was in the process of reviewing their Section 15 safeguards and we also had the opportunity to discuss the system that was in the process of being acquired to manage the interception work.

### 6.5.8 Home Office

Security Service and law enforcement interception warrants must pass through the National Security Unit (NSU) 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 April and October 2012. Lists of interception warrants current, extant and expired were provided to my office in good time to select sample warrants for these review visits. Staff also took the opportunity to discuss the planning and preparation for the 2012 London Olympics.

I was impressed with the staff I met who are undertaking an important quality assurance role on behalf of the Senior Official and the Home Secretary.

### 6.5.9 Scottish Police Forces, Scottish Drug Enforcement Agency (SCDEA) and Scottish Government

My formal inspection visits took place in May and November 2012 and were hosted by the Scottish Government. Prior to the inspection I selected a number of warrants from across the Scottish forces to review.

I received presentations from the relevant police forces in relation to specific interception warrants and, when necessary, was able to discuss the rationale behind the warrants with the officers concerned. The inspection was hosted by the staff involved in managing the warrantry for Scotland and preparing the interception warrants for signature by Scottish Ministers. The staff I met were diligent and fully aware of their obligations in relation to the legislation. I was briefed in relation to the work being undertaken to merge the Scottish police forces and SCDEA into Police Scotland from 1st April 2013.

### 6.5.10 Police Service of Northern Ireland (PSNI) and Northern Ireland Office (NIO)

My formal inspection visits of the PSNI took place in April and November 2012 and were hosted by the NIO. The NIO manages all of the lawful intercept warrants signed by the Secretary of State for Northern Ireland.

I selected a number of warrants to examine and was impressed with the quality of the warrants and level of scrutiny applied by the NIO.

I was provided with a national security and political update from senior NIO and PSNI staff.

### 6.5.11 Ministry of Defence (MoD)

My formal inspection visits at MoD took place in early May and November 2012. I was able to scrutinise the MoD interception warrants and was satisfied that they were properly authorised and up-to-date.

## 6.6 Meetings with the Secretaries of State

### 6.6.1 Meeting with Home Secretary

I met with the Home Secretary in January and December 2012 and matters related to MI5, HMRC, MET CTC and SOCA were discussed. The Home Secretary has the largest volume of warrants to authorise. I am satisfied that the Home Secretary takes great care before signing interception warrants that potentially infringe on the private lives of citizens. It is apparent that she takes time to read submissions, often requesting further information and updates from officials in relation to certain warrants.

We discussed the advancement in communications technology over my 6 years in office and I reinforced my broad support for legislative changes in order to keep pace with future technology, and that extra staff and technical resources would be needed if the Interception of Communications Commissioner takes on the extra oversight proposed by the draft Communications Data Bill. I outlined that the intercepting agencies and wider public authorities have responded well to my inspections.

We discussed the Governments proposal to place my prison inspections on a statutory footing. I outlined that we have always received co-operation from the prisons, but that I did support the proposal. The proposal would provide the opportunity to extend the arrangement to cover the Scottish prisons and the secure hospitals which are not currently inspected.

### 6.6.2 Meeting with Foreign Secretary

I met with the Foreign Secretary in December 2012 to discuss the discharge of my oversight role in relation to the intelligence agencies GCHQ and SIS for whom he is responsible.

It is evident that the Foreign Secretary takes his role very seriously and that he often questions the proportionality of the warrants and requests early reviews or renewals in particularly sensitive or intrusive cases.

### 6.6.3 Meeting with Northern Ireland Secretary

I met with the Secretary of State for Northern Ireland in December 2012. We discussed her warrantry role broadly and also had a general discussion around the increased threat in Northern Ireland, particularly to police officers.

### 6.6.4 Meeting with Scottish Ministers

I met the Scottish Cabinet Secretary for Justice during my inspection of the Scottish Police forces and Scottish Government in October 2012. He took the opportunity to discuss the forthcoming merger of the Scottish Police forces and the SCDEA into one Police Service, describing the likely structure of Police Scotland when it comes into being on 1st April 2013. He expressed satisfaction in relation to the information he received to support the warrants he signed. I took the opportunity to discuss my non-statutory prison inspection regime in relation to the interception of prisoners' communications and offered to provide more information on the regime. The Minister showed a genuine willingness to involve IOCCO in an inspection process and gave an undertaking to discuss the matter with the head of the Scottish Prison Service.

### 6.6.5 Meeting with Defence Secretary

I met with the Defence Secretary in December 2012. We had a very general discussion about the warrants that he signs and the responsibilities of the MoD more broadly.

## 6.7 Communication Service Providers (CSPs)

I have continued the practice as in previous years of making informal annual visits to communication 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, is for me to meet senior staff and individuals engaged in lawful interception and acquisition of communications data, in order to be briefed on changes to technology and working relationships between the intercepting agencies, public authorities and CSPs. The staff within the 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 the intercepting agencies. I have attempted where possible to resolve any difficulties that have arisen between the intercepting agencies, public authorities and CSPs. I also take the opportunity to discuss any errors / breaches in further detail. 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.

## 6.8 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 the Secretaries of State, I am able to form the view that all those involved act with integrity and in a highly ethical manner.

# 7. ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA (RIPA PART I, CHAPTER 2)

## 7.1 General Background to Types of Communications Data

There are three types of communications data gathered under RIPA Part I, Chapter 2. These are fully defined in RIPA but in summary;

- Subscriber Data relates to information held or obtained by a Communication 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 communication 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 2 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), Environment Agency 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 have been 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 1 Chapter 2 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. 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. If we talk specifically about the larger users - police forces, LEAs and intelligence agencies – and suppose that the number of applications is a third of the number of notices and authorisations, then it is reasonable to suggest that my inspectors randomly examine approximately 10% of the notices and authorisations that are issued/granted. I am satisfied that this level of random sampling gives a reliable picture. The inspectors ensure that the applications they examine cover a range of themes in order to accurately measure the level of compliance. My inspectors will continue to examine applications until they reach the point that they are satisfied that what they have examined is an accurate representation in relation to the public authority's level of compliance. Compliance is measured against the inspection baselines which are drawn from the Act and Code of Practice. Where an inspector does not reach this point in the time allocated for an inspection he will arrange to revisit the public authority to conclude the inspection. This has happened in the past, but rarely occurs, as the time allocated to each inspection is based around the overall number of requests.

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. I am providing more information this year in relation to how my inspectors' satisfy themselves of this in order to address a comment made by the Joint Committee on the Draft Communications Data Bill. It is important to understand that my inspectors look at each request on an individual, case by case basis. The inspectors examine the justifications that have been set out in the application. The necessity and proportionality tests for acquiring communications data are quite specific – in order to justify necessity under Section 22(2) the applicant must make the link between the crime / offence (or other purpose), the suspect, victim or witness; and the phone or communications address – in order to justify proportionality the applicant must explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation, provide a justification as to how the specific date / time periods requested are proportionate and consider, if relevant, whether the objective could be achieved through less intrusive means. Collateral intrusion must also be considered and any meaningful collateral intrusion described (for example, the extent to which the privacy of any individual may be infringed and why that intrusion is justified in the circumstance). The case must be made for each specific data request and the application supporting the request should stand on its own. My inspectors seek to ensure that all of the above matters have been considered. If the inspector has concerns that the tests have not been met, they will speak to the applicant and / or the DP. The inspector may also ask to see further supporting documentation (such as the case file, policy logs, operational book etc).

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. It is worth pointing out that if the inspectors identify an error / issue during the

random sampling which may impact on other applications, the public authority is tasked to identify the other applications which contain the same error / fault. Therefore, although the random sampling may only pick up one error, this will lead to all error instances of that type being investigated and reported.

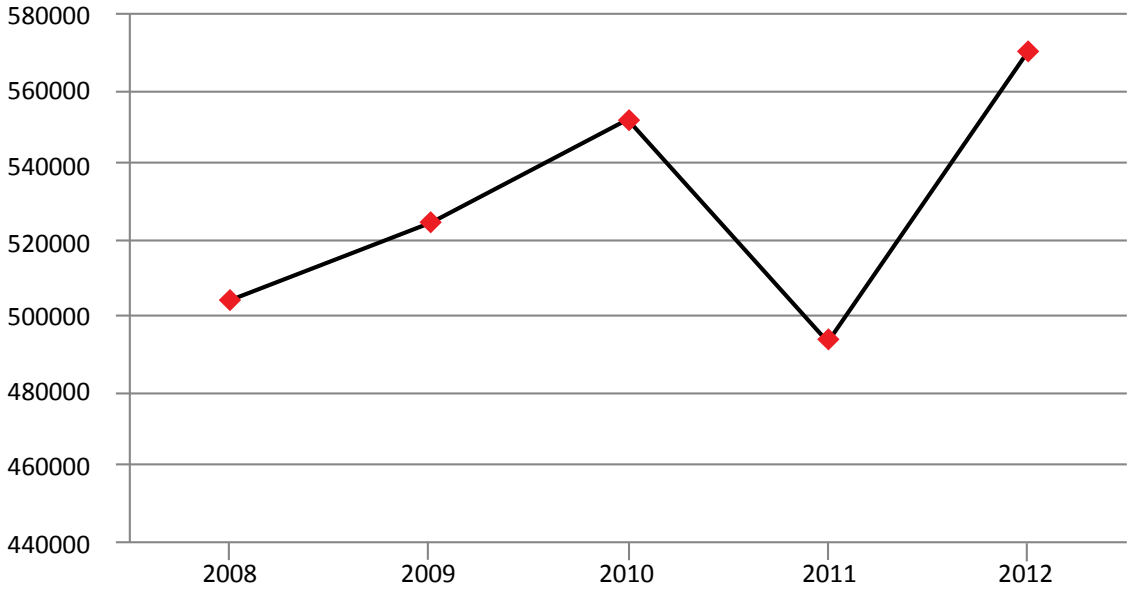
Following each inspection a detailed report is prepared and this outlines, inter alia, what level of compliance has been achieved with the Act and Code of Practice. I have sight of all of the inspection reports in order to discharge properly my oversight functions. Where necessary, an action plan will 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 570,135 notices and authorisations 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 7 illustrates that the number of requests submitted in 2012 represents an approximate 15% increase on 2011.

**Figure 7 – Number of Notices / Authorisations for Communications Data in the Previous 5 Year Period**

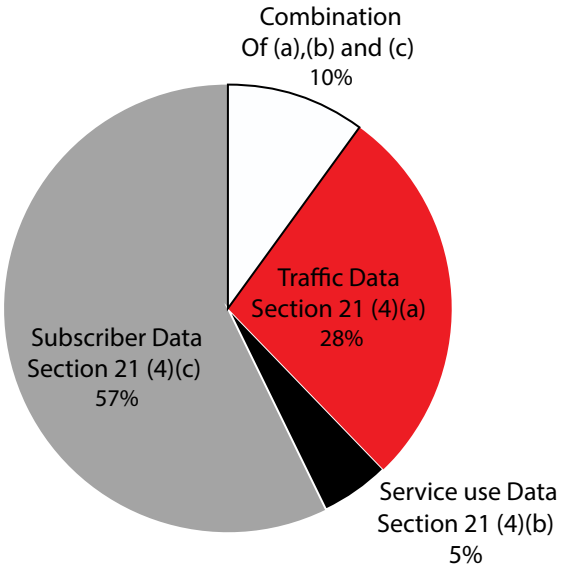



The statistics my office have collated show that 16 public authorities increased their requests for communications data on the previous year. The following explanations for the increase in demand have been provided by some of these public authorities; increase in training / awareness of applicants to request data; a number of large scale investigations; more internet data requests; more complex requests requiring notices / authorisations to be served on more than one CSP. The increase is also unsurprising considering the fact that the UK hosted the Olympic and Paralympic Games in 2012 and that communications data supported a number of operations undertaken to ensure the Games were safe.

The total number of applications is currently not reported to my office in the annual statistics as it is not a requirement of the record keeping provisions in the Code of Practice. An application will often result in more than one notice or authorisation being issued/granted, therefore the number of applications submitted will be less that the number of notices and authorisations. Conversely the number of individual items of data requested is likely to be higher than the number of notices and authorisations as multiple items of data may be requested on one authorisation or notice. The number of applications and the number of individual items of data requested would be useful figures to collect in future. It would also be useful to be able to determine the statutory purpose under which each request was made (i.e. in the interests of national security etc). The vast majority of the requests are made for the purpose of preventing or detecting crime or of preventing disorder. My Chief Inspector has been engaging with the Home Office to discuss how the record keeping and statistical requirements outlined in the Code of Practice might be amended in future to require more comprehensive statistics.

Figure 8 illustrates the breakdown of the communications data requests by type. Over half of the requests for communications data in the reporting year were for subscriber data under Section 21(4) (c), usually in the form of enquiries to ascertain the ownership of mobile phones. There has been no significant change to the percentage of requests for service use and traffic data, but the percentage of requests for 'combinations' of data have fallen by 7%.

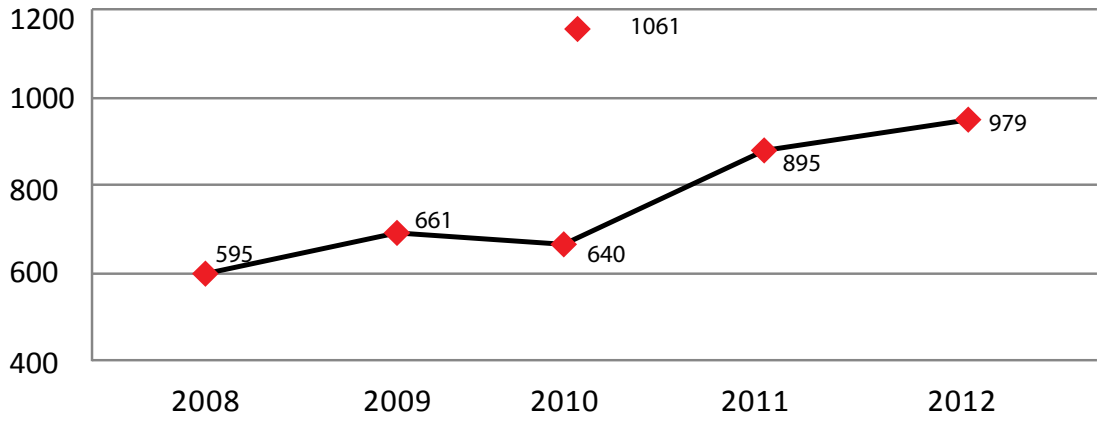
**Figure 8 – Breakdown of Communications Data Authorisations / Notices by Type**




## 7.4 Communications Data Errors

During the reporting year, 979 communications data errors were reported to my office by public authorities.

**Figure 9 - Number of Communications Data Errors Reported to the Commissioner in the Previous 5 Years**




This figure is higher than the previous year (895). However, as the number of requests has increased by 15% this year, the overall error percentage has actually reduced from 0.18% in 2011 to 0.17% in 2012. 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 979 errors were attributable to public authorities and 20% to CSPs. This percentage has remained static. This year my office has again collated management information in relation to the causes of the errors and as a result I am able to provide the same level of detail in this area.

**Figure 10 – Breakdown of Errors by Cause and Responsible Party**

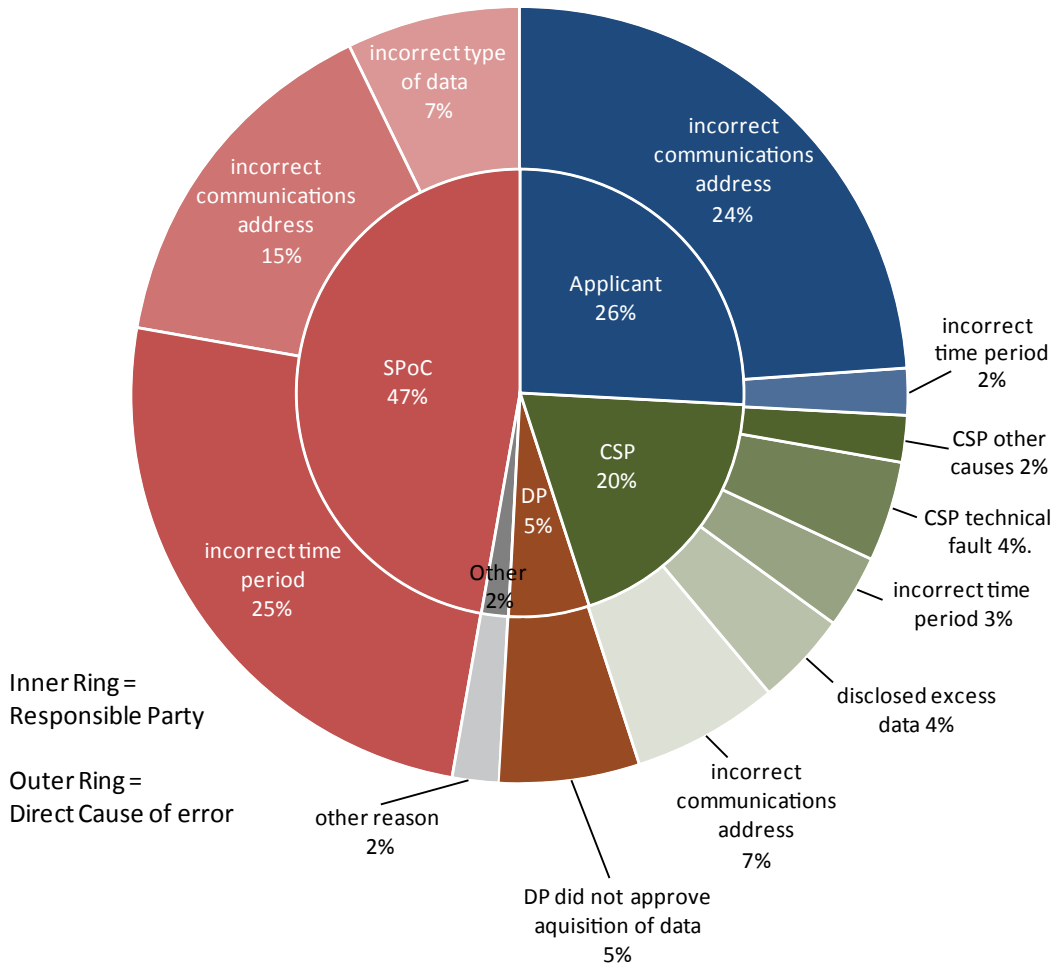



Figure 10 shows that 46% of the errors were caused either by the applicant, SPoC or CSP acquiring data on the incorrect communications address (an increase of 4 percentage points on 2011). This type of human error usually occurs due to the transposition of digits in telephone numbers or internet protocol (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. Regretfully in six separate cases this year, the mistake was not realised and action was taken by the police forces / law enforcement agencies on the

data received. In four of the cases the mistake was made by the public authority (either the applicant or SPoC acquiring data on either the incorrect communications address or time period) and in the remaining two the mistake was made by the CSP (disclosing data on the incorrect communications address). All of these cases were requests for internet data (Internet Protocol or node name resolutions). Regrettably, five of these errors had very significant consequences for six members of the public who were wrongly detained / accused of crimes as a result of the errors. The remaining one error also caused an intrusion into the privacy of an individual, as an address was mistakenly visited by police looking for a child who had threatened to commit self harm.

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. The public authorities and CSPs reported the errors promptly and provided my office with further information as requested. A number of measures have been put in place to prevent recurrence including; ensuring that all details are double checked, ensuring that SPoCs understand the functionalities that are unique to each CSP, issuing an aide memoire to relevant staff outlining the procedure to be followed and reiterating the checking process and potential consequences of errors. The College of Policing have also issued tradecraft advice to SPoCs in relation to IP resolutions, which include ensuring that more than one request is resolved where there are different IP addresses or dates / times of access. This will enable the results to be cross checked. Some of the public authorities have also put procedures in place to ensure the applicant also provides the source documentation with their application to resolve an IP address. This will enable the SPoC to double check the IP address, date / time of access and any time zone conversions. I am satisfied with the measures put in place by these public authorities and CSPs and hopefully this will prevent recurrence. Fortunately errors with such severe consequences are rare.

Figure 10 shows that 30% 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 increase of 6 percentage points on 2011). An additional 7% 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 number of SPoC errors has increased this year from 36% to 47% and this is concerning. The Senior Responsible Officers (SROs) are responsible for overseeing the reporting of errors to my office and the implementation of processes to minimise repetition. My inspectors are satisfied that they do this.

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.

Furthermore, some errors can occur due to technical faults on the various systems used to acquire communications data. Unfortunately such system faults will generally persist until they are discovered and fixed. This year I was notified of one such system fault by a CSP. The CSP

reported that the fault may have resulted in the incorrect data (either false positives or false negatives) being disclosed to public authorities in response to IP resolution requests. The CSP initiated an investigation into the matter immediately and provided regular updates in relation to the progress made in identifying whether any errors had occurred. Thousands of disclosure requests were manually checked by the CSP and fortunately the error ratio was very low, with only 39 errors discovered in total. The errors related to requests submitted by 14 different public authorities and the CSP ensured that the public authorities were informed as soon as the errors were identified and that the correct results were subsequently disclosed.

My office conducted an investigation into the impact of the errors. Fortunately the majority of the results had not yet been acted on or had already been disregarded by the public authorities as they did not relate to individuals known to their investigations. However in one case where a false negative (i.e. no data) was originally provided, the subsequent positive disclosure led to a suspect being identified and arrested for the possession of indecent images of children. In a second case where a false negative was originally provided, the subsequent positive disclosure led to two persons receiving warnings under the Harassment Act. This highlights how critical communications data is to some criminal investigations and that without it, they cannot be progressed.

I attended two meetings with the CSP in relation to the errors during which I was provided with a technical briefing in relation to the errors, the progress and subsequent result of the investigation and the measures put in place to prevent recurrence. I am very grateful for the open and transparent approach that the CSP adopted in this matter. Adequate resources were deployed and the staff worked diligently to identify the disclosures that had been affected, report the error instances to my office and to the public authorities, and put in place the necessary corrective action to prevent recurrence. I am satisfied that the CSP complied with their obligation under Section 58 of RIPA and Paragraph 6.19 of the Code of Practice.

I can report that 33 of the 979 errors were first identified by my inspectors during their 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. All of these error were subsequently reported.

It is important to make the point that although there is a drive to design automated systems to reduce the amount of double keying and resultant human error that occurs, it is crucial for such systems to be sufficiently tested and to be subject to ongoing data quality checks to ensure they are functioning effectively. Otherwise there is a distinct possibility that the human errors will simply be replaced by technical system errors.

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 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.

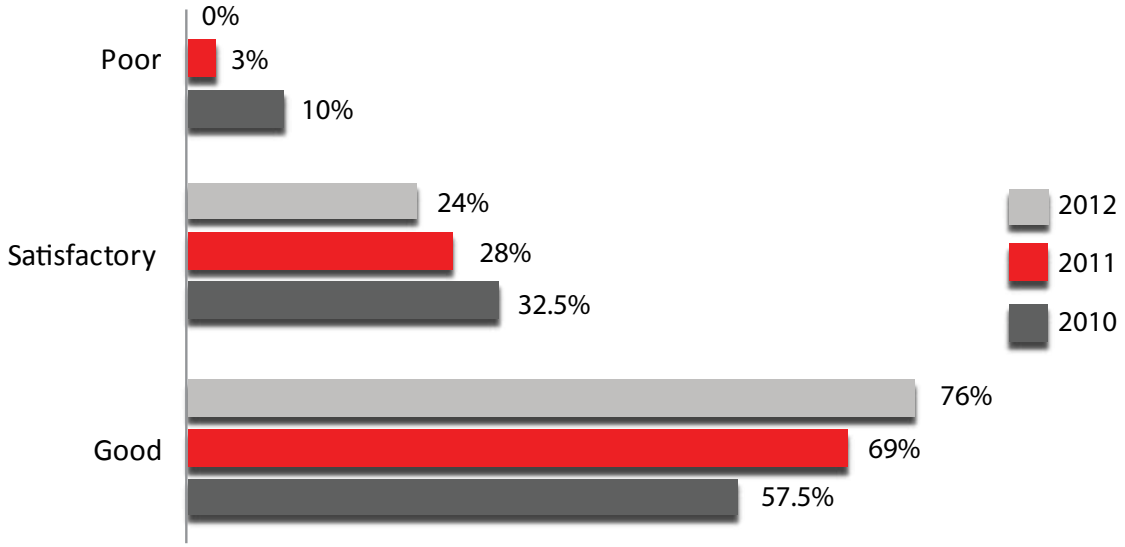
### 7.5.1 Police Forces and Law Enforcement Agencies (LEAs)

There are 43 police forces in England & Wales; 8 police forces in Scotland (to become 1 in April 2013); and the Police Service of Northern Ireland (PSNI). These 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. LEAs comprise Her Majesty's Revenue and Customs (HMRC); the Serious Organised Crime Agency (SOCA); the Scottish Crime and Drug Enforcement Agency (SCDEA) (to become part of Police Scotland in April 2013); United Kingdom Border Agency (UKBA); and the Child Exploitation & Online Protection Centre (CEOP) which is part of SOCA.

In 2012 my inspection team conducted 42 inspections of police forces and LEAs. 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 11 illustrates that 76% of the police forces and LEAs achieved a good level of compliance overall. This represents a 7 percentage point 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. In addition for the first time since the inspection regime started in 2005, none of the police forces emerged from their inspections with a poor level of compliance.

**Figure 11 – Comparison of Police Force and LEA Inspection Results, 2010 - 2012**

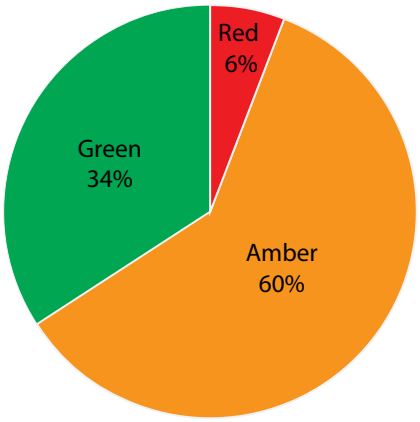



My inspectors found that the vast majority of police forces and law enforcement agencies had fully implemented their previous recommendations. As a consequence, an overwhelming number had either improved or sustained their good level of compliance with the Act and Code of Practice.

*"For the first time since the inspection regime started in 2005, none of the police forces emerged from their inspections with a poor level of compliance."*

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 237 recommendations were made by my inspectors during the 42 police force and LEAs inspections, which is again an average of 6 recommendations per public authority. Figure 12 shows the breakdown of recommendations by colour.

**Figure 12 – Recommendations from 2012 Police Force and LEA Inspections**




This year 6% of the recommendations represented serious non-compliance with the Act and Code of Practice and this is an increase on 2011 by 2 percentage points. Red recommendations were given to 13 different police forces. However, all but one of these police forces only received a red recommendation in relation to one compliance baseline and therefore ultimately these police forces were deemed to have a good or satisfactory level of compliance overall. The red recommendations fitted into two distinct areas; DP approvals (written and oral) and the procedures surrounding the acquisition of 'related' communications data. The following paragraphs describe the findings of the inspections in more detail and in cases where relevant, refer to the recommendations emanating from the inspections.

*"My inspectors did challenge the justifications for acquiring the data in a small number of cases as they were not satisfied that the requests were proportionate based on the information contained in the applications"*

All of the police forces and LEAs that were inspected during the reporting year were consistently producing good or satisfactory quality applications. My inspectors were satisfied that the acquisition of the data was necessary and proportionate in the vast majority of cases. My inspectors did challenge the justifications for acquiring the data in a small number of cases as they were not satisfied that the requests were proportionate based on the information contained in the applications. These cases were mainly investigations where data had been acquired for lengthy time periods without sufficient justification. In these cases my inspectors asked the relevant applicants and DPs to justify the requests and in some cases they examined further documentation, for example, the communications data strategy. On the basis of the further information provided my inspectors were able to conclude that the requests were not disproportionate, but rather the applicants had failed to justify properly the time periods in their applications. In these cases advice was provided to the effect that it is an established principle that an application for communications data must stand on its own and sufficient information must be included to enable the DP to make a decision whether the request is necessary and proportionate. Amber recommendations were given to the police forces to ensure applicants properly justify the principle of proportionality in their applications.

A number of CSP disclosures were randomly checked against the records kept by the police forces and LEAs, 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.

The evidence shows that the SPoC process is a robust safeguard. The SPoCs are exercising their guardian and gatekeeper function responsibly and my inspectors saw ample evidence of the SPoCs challenging applicants and DPs in cases where they felt the requirements of the Act had not been met. They also saw ample examples of the SPoCs assisting the DPs to discharge their statutory duties responsibly. 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 was concerned to report that 20% of the police forces, LEAs inspected in 2011 had a lack of staff in their SPoC unit. Regrettably this year my inspectors found that 19% of the police forces and LEAs were experiencing serious backlogs in dealing with applications due to a lack of staff. There is a risk that applicants in these public authorities 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. Amber recommendations have been made for these public authorities to take the necessary steps to ensure that they have sufficient trained staff. Furthermore, green recommendations were given to 2 police forces for the SROs to keep the staffing under continuous review as there appeared to be little resilience. During the reporting year some of the police forces have taken advantage of the collaboration provisions in the Policing and Crime Act 2009. It is likely that in the future more police forces will brigade their SPoC resources into a region and this may assist to resolve some of the resilience issues, so long as the regional SPoCs are sufficiently resourced.

*"The evidence shows that the SPoC process is a robust safeguard……..My inspectors saw ample evidence of the SPoCs challenging applicants and DPs in cases where they felt the requirements of the Act had not been met"*

My inspectors concluded that the DPs are generally discharging their statutory duties responsibly. The DPs in 74% of the police forces and LEAs were found to be recording their considerations to a consistently good standard. It was quite clear that the majority of the 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 show that just under 5500 applications were rejected in 2012 by DPs in police forces and LEAs. If we suppose that the total number of applications is a third of the number of notices and authorisations, then it is reasonable to suggest that approximately 3% of all applications were rejected by the DPs. It is important to make the point that a much larger percentage of applications will have been refused or returned to the applicants for further development by the SPoCs prior to them even reaching the DPs. This would be a useful figure to collect in future, but it is not currently a requirement of the record keeping provisons in the Code of Practice.

However the 74% reported is a reduction from last year when I reported that the DPs in 88% of the police forces and LEAs were meeting this standard. Although this percentage should be treated with caution as the public authorities being inspected are not the same every year, there were serious compliance issues identified in this area in a small number of the police forces which resulted in red recommendations being made. In three police forces, my inspectors were concerned to find that a number of the DPs had not actually recorded any written considerations when approving some of the applications and this constitutes non-compliance with Paragraph 3.7 of the Code of Practice. It was however clear in these cases that the DPs had actually approved the requests.

My inspectors concluded that there was a good level of objectivity and independence in the approvals process within specialist departments such as Special Branch (SB) and Professional Standards Departments (PSDs), or if not, they found that Paragraph 3.11 of the Code of Practice was being complied with. However, some compliance issues were identified in this area of the process which resulted in amber recommendations. First, in 7 of the police forces the PSD applicants were not naming the subjects of the investigation. Second, in 9 of the police forces the PSD or SB applicants had not specified the crime / offence under investigation. These two points are key parts of the necessity test and in these cases my inspectors challenged the necessity of the requests. My inspectors were informed that in some of the instances separate verbal briefings had been provided to DPs. This is unsatisfactory and there was no evidence of what the briefings consisted of. My inspectors were provided with supplementary information supporting the applications which led them to conclude that the requests met the necessity test. However, as already outlined, it is an established principle that an application for communications data must stand on its own and sufficient information must be included to enable the DP to make a decision whether the request is necessary and proportionate. Amber recommendations were made in this area to ensure that applicants properly justify the principle of necessity in their applications.

*"it is an established principle that an application for communications data must stand on its own and sufficient information must be included to enable the DP to make a decision whether the request is necessary and proportionate"*

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 frequently saves lives. 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 39,092 requests were orally approved which represents an increase on last year's figure of 35,109. Again 90% of the police forces and LEAs were found to be achieving a good or satisfactory level of compliance in relation to the overall management of the urgent oral process and the quality of the record keeping.

Last year I reported that 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. My inspectors identified one such case this year in a police force. In this case the DP had not given the requisite authority for the subsequent data that was acquired to be obtained. Although this instance represents serious non-compliance, I am satisfied that it was not a wilful or reckless failure. It is also important to recognise that it occurred in relation to an exceptionally urgent case and that the persons involved in the process were working under immense pressure in an attempt to save a life. Nevertheless, it is still very important to ensure that the correct process is always applied and that the data is acquired in accordance with the law. A red recommendation was given to the police force in this area.

*"90% of the police forces and law enforcement agencies were found to be achieving a good or satisfactory level of compliance in relation to the overall management of the urgent oral process and the quality of the record keeping."*

My inspectors again found that a number of police forces and LEAs 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. This misunderstanding resulted in red recommendations being given to 7 police forces. 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. This part of the inspection process was not introduced until 2010 and all of the police forces and LEAs will now have received an inspection in this area and this should ensure improved compliance in future.

It is evident that police forces and LEAs are making good use of communications data as a powerful investigative tool, primarily to prevent and detect crime and disorder. It is also apparent that communications data plays a crucial role in the successful outcome of prosecutions and often it is the primary reason why offenders plead guilty. SPoCs throughout the UK continue to provide a valuable service to the investigation teams and often they make a significant contribution to the successful outcome of operations. I would like to highlight a few examples of how communications data is used by police forces and LEAs 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 4 – Leicestershire Police – Operation Kanzu

This investigation into the attempted robbery of a Post Office effectively used communications data to link the offender to the crime. The Postmaster had been followed from the Post Office to a location near to his home in Nottingham. Having stopped to make a call on his mobile phone, he was dragged out of his car at gunpoint by two men who threatened to kill his wife and family if he didn't assist them to gain entry into the Post Office. The recipient of the phone call made by the Postmaster heard the scuffle and alerted the police. Uniformed officers were sent to the Post Office and found the distressed Postmaster in the rear of a stolen car. Two men fled from the scene but evaded capture. Forensic examination of the stolen car revealed a possible suspect. A communications data

strategy was devised. A mobile telephone was identified for the suspect from overt police intelligence systems. Location data was acquired and analysis of this demonstrated that the suspect had been in the vicinity of the Post Office and had then travelled to the area of the abduction before returning to the vicinity of the Post Office. This was overlaid with location data from the Postmaster's phone which showed similar movements immediately before and after the abduction. The location data also showed that the suspect had been in the vicinity of where the car was stolen the day before. Seven applications were submitted during this investigation and the communications data that was acquired directly led to the arrest of the suspect. A search of his premises revealed a fake firearm together with gloves and a balaclava worn at the time of the abduction. The communications data was pivotal to the investigation and excellent quality analytical charts were prepared for Court. In June 2012 at Leicester Crown Court, the offender pleaded guilty to attempted robbery and kidnapping and was sentenced to 8 years imprisonment. He also pleaded guilty to firearms offences and was sentenced to 4 years imprisonment to be served concurrently.

**Case Study 5 – South Yorkshire Police - Operation Anzac**

This investigation commenced following the report of the suspicious death of Ildiko Dohany, who was found beside her car in September 2011. Three suspects were arrested close to the scene and a number of mobile phones belonging to the victim and the suspects were seized for forensic examination. The computers belonging to the victim and a suspect were also examined. Initially, incoming and outgoing call data and location data was acquired on the mobile phones attributed to the victim and suspects. The analysis of communications data was crucial in discrediting the account given by the main suspect regarding his and the victim's movements. It was suspected that the suspect used the victim's phone after her death to support his false version of events. The analysis of the communications data also assisted the team to acquire Automatic Number Plate Recognition data and CCTV which covered the movements of the victim's car and the suspects on foot. Furthermore, analysis of the suspect's contact with the victim in the weeks before her death revealed a pattern of behaviour where he was accessing the stored email communications between the victim and her boyfriend. Following repetitive reading of these emails, the suspect then made telephone contact with the victim. In June 2012 at Sheffield Crown Court, Martin Vernasky denied murdering Ildiko Dohany, but was found guilty of manslaughter and sentenced to six years imprisonment.

## 7.5.2 Intelligence Agencies

The intelligence agencies are subject to the same type of inspection methodology and scrutiny as police forces and LEAs. 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. 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. GCHQ and SIS had updated and streamlined a number of their systems and procedures in line with recommendations from their 2011 inspections. These changes reduced unnecessary bureaucracy and improved the systems and processes for acquiring communications data in these agencies.

### 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.

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.

> *"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."*

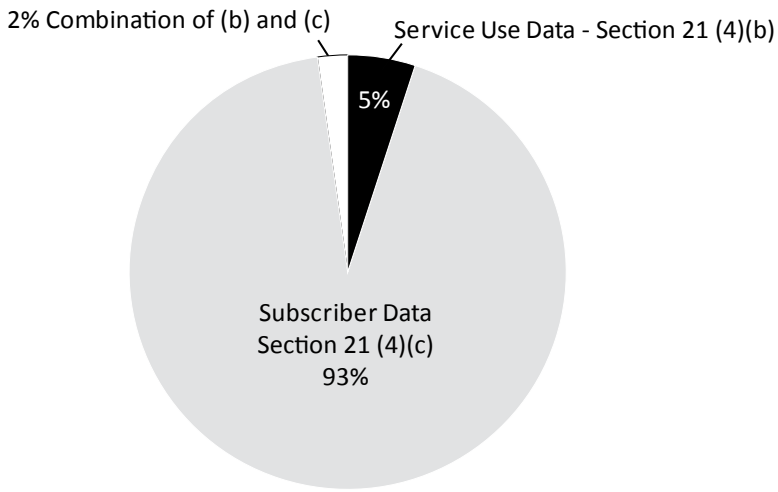
By comparison with police forces and LEAs, local authorities make very limited use of their powers to acquire communications data. During the period covered by this report 160 local authorities notified me they had made use of their powers to acquire communications data, and between them they made a total of 2605 requests. This is an increase from the previous year's figures (141 local authorities, 2130 requests).

To put this last figure into context, it represents less than 0.5 % of all communications data requests submitted by public authorities. 73% of the 160 local authorities made less than 20 requests in the reporting period and 53% made less than 10 requests. These percentages are very similar to those in the previous two reporting years.

> *"73% of the 160 local authorities [that made use of their powers] made less than 20 requests and 53% made less than 10 requests"*

Figure 13 illustrates that 93% of the 2605 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 unknown suspects, thought to be responsible for particular criminal offences. This year a quarter of the 160 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 7% of requests.

**Figure 13 – 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. 129 of the 160 local authorities who used their powers this year reported that they are now submitting their requests through NAFN. In addition a number of local authorities who did not submit applications in the reporting year have also subscribed to the NAFN SPoC Service. Approximately 88% of the 2605 requests made in 2012 were managed by the NAFN SPoC Service and this is a further increase from last year (70%).

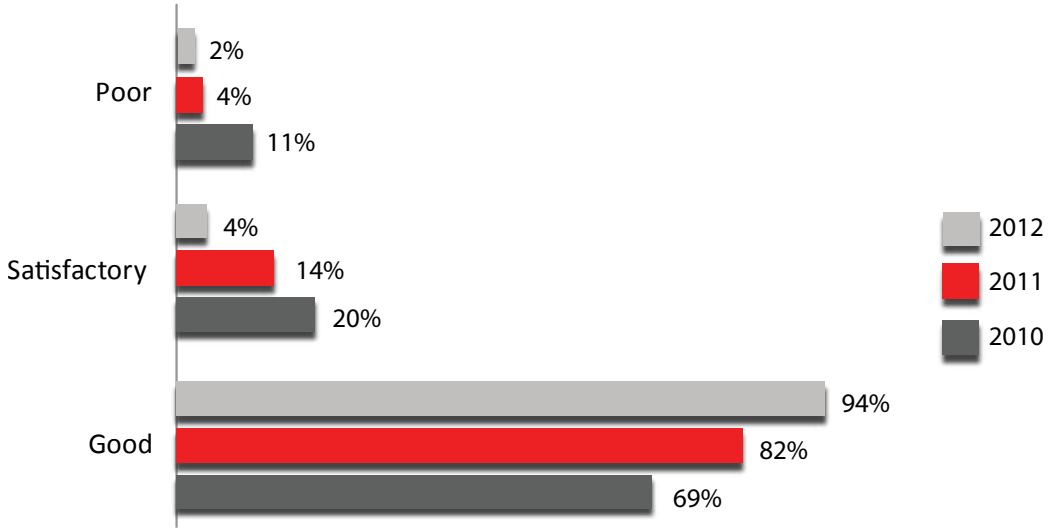
*"Approximately 88% of the 2605 requests [made by local authorities] were managed by the NAFN SPoC Service"*

NAFN was inspected once during the reporting year. During the NAFN inspection my inspectors examined approximately half of the communications data requests that had been submitted in the period being inspected. 126 individual local authorities had submitted applications in that period and the inspectors ensured that they examined applications relating to each individual local authority. I am pleased to report that NAFN again emerged very well from their inspection. The SPoCs at NAFN are providing an excellent service and are ensuring that local authorities act in an informed and lawful manner when acquiring communications data. Overall NAFN is achieving a good level of compliance with the Act and Code of Practice on behalf of its local authority members.

During the reporting year 38 inspections were also conducted at local authorities who were not making use of NAFN at that time and for 18 of these local authorities it was their first inspection. Only 8 of the local authorities who reported using their powers in 2012 (but not through NAFN) were not inspected by my team during the year.

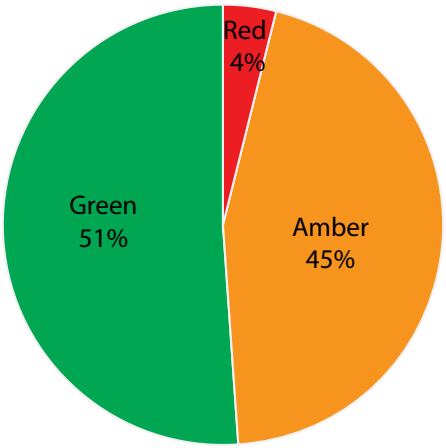
Figure 14 illustrates that 94% of the local authorities inspected achieved a good level of compliance with the Act and Code of Practice which is an increase of 12% on the previous year. These percentages should be treated with caution as the public authorities being inspected are not the same every year.

**Figure 14 – Comparison of Local Authority Inspection Results, 2010 to 2012**




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 171 recommendations were made by my inspectors during the 39 local authority inspections and this is an average of 4 recommendations per public authority (if all NAFN users are treated as one). This is a 66% reduction on the number of recommendations emanating from the 2011 inspections. Figure 15 shows the breakdown of recommendations by colour.

**Figure 15 – Recommendations from 2012 Local Authority Inspections**




This year 4% of the recommendations represented serious non-compliance with the Act and Code of Practice. These red recommendations were made in relation to 7 separate local authorities. 4 of these local authorities emerged poorly from their inspections overall. It should be recognised that it was the first time that these four local authorities had been inspected. I am pleased to report that two of these local authorities are now using the NAFN SPoC to manage their communications data requests and the remaining two did not use their powers at all in 2012. The red recommendations fell into two areas; DPs approvals and record keeping requirements and will be covered later in this section.

The vast majority of the local authorities that were inspected during the reporting year were completing their applications to a good or satisfactory standard. My inspectors did challenge the justifications for acquiring the data in a very small number of cases as they were not satisfied that the requests were necessary and / or proportionate based on the information contained in them. During the inspections the investigations were discussed in more detail with the applicants and / or DPs and in some instances the case files for the investigations were examined. From this supplementary information the inspectors were satisfied that the requests were submitted in relation to criminal offences which the public authority has a statutory duty to investigate and that the objective justified the potential intrusion. However it is now an established principle that an application for communications data should stand on its own and sufficient information must be included to enable the DP to make a decision whether the request is necessary and proportionate. 11 of the local authorities were not actually using the latest version of the Home Office and ACPO DCG application form template and this explained why some of the salient points were not covered. Amber recommendations were given to 14 of the local authorities to assist the applicants to improve further the necessity and / or proportionality considerations in their applications.

*"My inspectors did challenge the justifications for acquiring the data in a very small number of cases as they were not satisfied that the requests were necessary and / or proportionate based on the information contained in them."*

My inspectors found that the DPs were generally discharging their statutory duties responsibly. The statistics provided to my office this year show that 55 applications were rejected by the DPs in 2012. The majority were found to be completing their written considerations to a good standard. However, my inspectors found that in two 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 however it was clear they had seen and approved the applications. These local authorities received red recommendations in this area and 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 one local authority two communications data requests (submitted on one application) were not approved by a person of sufficient seniority to act as a DP. Regrettably this data was not acquired in accordance with the law. In two other local authorities, the record keeping requirements outlined in Paragraph 6.1 of the Code of Practice had not been complied with and as a result there was no record of the DPs approvals, or in one instance, of an application form being completed. In one of these instances, the SPoC had also acted as the DP (which is permissible) and therefore it was clear that an approval had been given to acquire the data.

*"My inspectors found that the [local authority] DPs were generally discharging their statutory duties responsibly."*

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 both of these instances the traffic data was disclosed by the CSPs and as a result the local authorities obtained data to which they were not lawfully entitled. In one of the instances it was not actually necessary to acquire the traffic data (incoming call data) as the objective was to prove contact between three known individuals. Acquiring outgoing call data under Section 21(4)(b) in relation to the three individuals would have achieved the objective. The inspectors were satisfied that these two instances were genuine mistakes, but it does emphasise the importance of the SPoC being appropriately trained as well as the CSPs role in checking the requests they receive.

A number of the local authorities inspected were still not aware that it is the statutory duty of the DP to issue Section 22(4) Notices, despite the fact that I have raised this point in my previous two annual reports. 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.

Last year I reported that my inspectors identified a large number of reportable errors during the 2011 local authority inspections that had not been notified to my office. I am very pleased to report that this was certainly not the case in 2012 as only 7 errors were discovered by my inspectors. It is important to make the point that the serious compliance issues relate to a very

small number of local authorities (just 7 of the 164 local authorities inspected). Overall the picture is very positive, with the number of local authorities achieving a good level of compliance increasing by 12 percentage points, and the number of recommendations emanating from the local authority inspections reducing by more than 50%.

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. No instances of local authorities inappropriately using their powers (i.e. not for the purpose of preventing and/or detecting crime) were identified during the 2012 inspections. 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.

*"Overall the picture is very positive, with the number of local authorities achieving a good level of compliance increasing by 12 percentage points, and the number of recommendations emanating from the local authority inspections reducing by more than 50%"*

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 some further examples of how communications data is used by local authorities as this may provide a better understanding of its importance to the criminal investigations that local authorities undertake.

### Case Study 6 – North Yorkshire Council use of Communications Data – Operation Violet

This operation commenced in May 2009 when elderly residents in Thirsk, North Yorkshire complained about gardening work that had been carried out following cold calls by doorstep traders. The victims had been charged excessive prices for small amounts of gardening work. The investigation revealed the lengths to which the gang would go to press the most vulnerable and elderly to pay for work which was rarely undertaken. One 85 year old was pressurised to part with £52,000. Another elderly lady was defrauded out of more than £23,000. In some cases the gang made repeated visits to victims, extorting money based on false claims. Communications data was used to link individual members of the gang to specific offences. Some of the victims had telephone numbers noted on flyers and in diaries, calendars and address books. Subscriber checks were able to link those numbers to some of the gang. Outgoing call data proved that the telephones seized from the defendants had been used to call many of the victims. All of the defendants pleaded guilty to various offences including conspiracy to defraud, money laundering and theft at Teesside Crown Court in May and July 2011. The defendants were sentenced to a total of 25 years imprisonment, the longest term being 7 years 8 months.

### Case Study 7 – North Yorkshire Council use of Communications Data – Operation Zinnia

Communications data was used effectively in relation to this car clocking investigation. The vehicles were purchased by the offenders (4 brothers) at local car auctions and the mileages were reduced dramatically. In one case a car had its mileage reduced by over 200,000 miles. The offenders sold the cars from their home addresses using multiple trading names. Unsuspecting consumers purchased the cars after seeing them advertised on the Autotrader website. In some instances, false service histories were also supplied with the cars. Two of the offenders denied being involved in some of the sales and subscriber checks were used to show that the phone numbers in particular car adverts were linked to those individuals. Subscriber checks were also used to identify the users of various email addresses connected to the placing of adverts. One of the brothers was also charged with perverting the course of justice, together with a fifth male (who had come forward to trading standards and falsely claimed he was responsible for the sales). The perverting the course of justice offences were proved by a text message recovered from a seized phone (and subsequent subscriber check which showed who sent / received the message). The four brothers were prosecuted for conspiracy to commit fraud. One of the brothers was also prosecuted for money laundering, and he and the fifth male were prosecuted for perverting the course of justice. All five individuals pleaded guilty and were sentenced at Leeds Crown Court on 14th November 2011. The principal defendant received 18 months imprisonment. His three brothers were sentenced to 12 month imprisonments, suspended for 3 years, and were ordered to carry out 200 hours unpaid community work. The fifth male was sentenced to 12 months imprisonment, suspended for 2 years, and was ordered to carry out 100 hours unpaid community work. A proceeds of crime act confiscation hearing is underway to confiscate assets held by the defendants as a result of their criminal conduct. Any monies recovered will be used to compensate the victims in the case.

## 7.5.4 Other Public Authorities

There is 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 LEAs, these Other public authorities make very limited use of their powers to acquire communications data. During the period covered by this report 25 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 2379 requests, a decrease of 31% on the previous year. To put this figure in context, it represents just 0.4% of all communications data requests submitted by public authorities.

During the course of the reporting year inspections were carried out at 21 of these public authorities. Figure 16 lists the public authorities who reported using their powers in 2012.

**Figure 16 All Other Public Authorities who reported using their powers in 2012**

| Inspected in 2012 (and used powers) | Inspected in 2012 (but did not use powers) |
|---|---|
| Child Maintenance & Enforcement Commission | NHS Scotland Counter Fraud Services |
| Department for Transport - Marine Accident Investigation Branch | Merseyside Fire and Rescue Authority |
| Department for Transport - Rail Accident Investigation Branch | Cambridgeshire Fire and Rescue Service |
| Department of Health – Medicines and Healthcare Products Regulatory Agency (MHRA) | |
| Department of the Environment (Northern Ireland) | |
| Environment Agency | |
| Financial Services Authority (FSA) | |
| Gambling Commission | |
| Gangmasters Licensing Authority | |
| Independent Police Complaints Commission (IPCC) | |
| Information Commissioner's Office | **Not Inspected in 2012 (but used powers)** |
| Maritime & Coastguard Agency | Department for Transport - Air Accident Investigation Branch |
| National Offender Management Service (NOMS) | Department of Business, Innovation & Skills |
| Department of Enterprise, Trade and Investment - NI TSS | Dorset Fire & Rescue Service |
| Office of Communications | Health & Safety Executive |
| Office of Fair Trading | NHS Counter Fraud & Security Management Service |
| Police Ombudsman for Northern Ireland | Royal Mail |
| Serious Fraud Office | |

Once again the largest user by far was the Financial Services Authority (FSA) who made 1302 of the 2379 requests (approx 55%). The second largest user only made 220 requests. This year 81% of the requests were submitted by just 4 public authorities; the Financial Services Authority, the National Offender Management Service (NOMS), the Department of Enterprise, Trade and Investment (Northern Ireland Trading Standards Service) and the Department of Health (Medicines Healthcare and Regulatory Services).

60% of the 25 public authorities who reported using their powers made less than 30 requests in the reporting period. Figure 17 illustrates that 52% of the 2379 requests were for subscriber data under Section 21(4) (c). 15 of the 25 public authorities acquired service use data under Section 21(4) (b), 9 acquired traffic data under Section 21(4) (a) and 16 acquired a combination of data types.

**Figure 17 – Percentage of Communications Data Requests by Type**

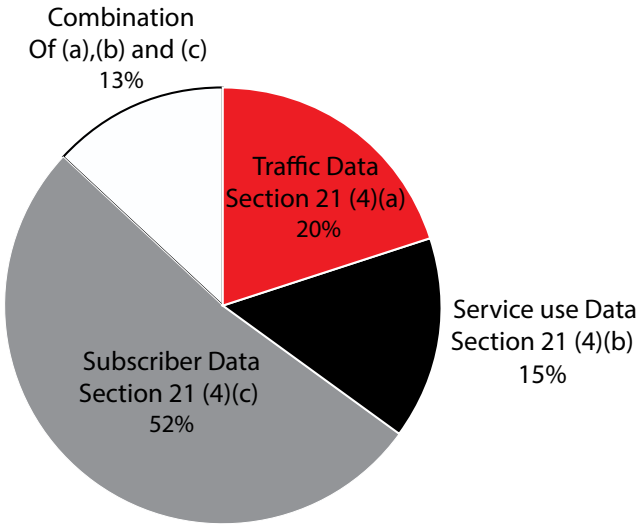
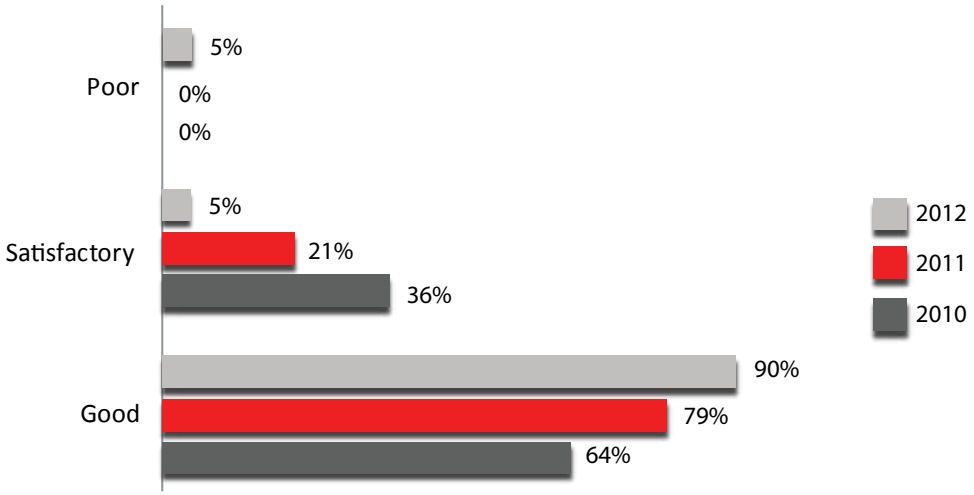


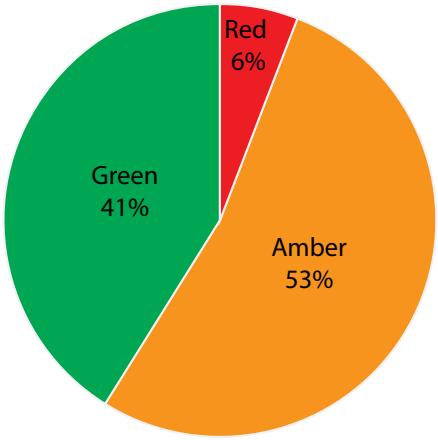

Figure 18 illustrates that 90% of the Other public authorities inspected achieved a good level of compliance with the Act and Code of Practice and this represents an 11 percentage point increase on last year. However this percentage should be treated with caution as the public authorities being inspected 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 18 – Comparison of Other Public Authority Inspection Results, 2010 to 2012




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 85 recommendations were made by my inspectors during the Other public authority inspections and this is an average of 4 recommendations per public authority. Figure 19 shows the breakdown of recommendations by colour.

## Figure 19 – Recommendations from 2012 Other Public Authority Inspections



This year 6% of the recommendations represented serious non-compliance with the Act and Code of Practice. Figure 18 shows that regrettably one public authority emerged poorly from their inspection and I can report that this was a Fire and Rescue Authority. 4 of the 5 red recommendations actually related to this one public authority. It was the first inspection of the authority as although they reported using their powers infrequently in 2006 and 2007, no data had been acquired between 2008 and 2010. The 2012 inspection was planned in response to statistics provided at the end of 2011 which indicated some further usage. My inspector identified serious non-compliance with the Act and CoP during this inspection which stemmed from the fact that the record keeping requirements outlined in Paragraph 6.1 of the Code of Practice had not been complied with (copies of applications and DPs approvals not retained). Due to the lack of documentation and records, it was not possible for my inspector to be satisfied firstly that the acquisition of communications data satisfied the principles of necessity and proportionality or secondly that the communications data had been acquired lawfully. It was not even clear if any data had been acquired by the public authority as there were no records in relation to any CSP disclosures. I concluded that although the public authority's conduct bordered on reckless, they had not wilfully breached the legislation. Furthermore the public authority assured me of their desire to achieve compliance with their obligations under Part I Chapter 2 of RIPA in future. The inspection report was hard hitting and was difficult for the public authority to accept, however I understand the recommendations from the inspection have now been addressed. I assured the public authority that my office would continue to work positively with them to ensure compliance.

*"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 2 of RIPA were not used for those purposes."*

This year more than half of the recommendations were amber. These recommendations fell into 4 key areas; Applicant, SPoC, DPs and Notices. Amber recommendations were made to assist the public authorities to tighten their procedures in these areas and / or to improve administrative compliance issues. These recommendations will be covered later in this section of the report.

90% of the public authorities that were inspected during the reporting year were completing their applications to a good or satisfactory standard. In a minority of cases the inspectors had to discuss the justifications further with applicants or DPs or examine supplementary evidence in order to be satisfied that the requests were necessary and proportionate. In these cases they concluded that there was still room for applicants to improve on the quality of their applications to ensure they can stand alone. The inspections confirmed that the public authorities inspected 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 2 of RIPA were not used for those purposes.

Overall my inspectors were satisfied that the SPoCs were ensuring that their public authorities acted in an informed and lawful manner when acquiring communications data. Amber

recommendations were given to a small number of the public authorities for the SPoCs to ensure they provide a more robust guardian and gatekeeper function with regard to the quality of the applications. Two of the public authorities also received amber recommendations to tighten the audit trail of the process.

My inspectors concluded that the DPs are generally discharging their statutory duties responsibly. The DPs in 86% of the Other public authorities were found to be recording their considerations to a consistently good standard. It was quite clear that the majority of the 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 show that 76 applications were rejected by the DPs in 2012.

In 3 of the inspections my inspectors concluded that some of the applications had not been approved in a timely fashion by the DPs. For a number of reasons it is vitally important that applications are approved speedily, otherwise this may have an adverse impact upon the progress of the investigations. Furthermore, after lengthy periods of time it must be questionable if the necessity and proportionality justifications are still valid. 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 are equally pertinent to some of these inspections and technical breaches were again found in this aspect of the process during 7 of the inspections. Amber recommendations were made in these two areas.

This year 41% 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. For example, to introduce the streamlining procedures outlined in Paragraphs 3.30 to 3.32 of the Code of Practice.

I would like to highlight two further investigations 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 8 – NHS Scotland - Use of Communications Data

Communications data was used very effectively in the investigation of several online accounts that had been discovered advertising more than £80,000 worth of stolen hospital and surgical supplies. Amongst items for sale were cranial drill-bits used in neurosurgery. Communications data was acquired in relation to Internet Protocol (IP) addresses and email addresses from the online accounts and transactions. The subscriber data acquired enabled investigators to identify four suspects at two addresses linked to the online seller accounts. Two of the suspects were employed by the NHS, one as an operating theatre technician. Search warrants were obtained for both of the addresses which resulted in the recovery of stolen property to the value of £28,000. Computers and laptops were seized and analysed, showing that the scope of the selling network was worldwide. The main suspect pled guilty to theft and was sentenced to 18 months imprisonment.

**Case Study 9 – Medicines and Healthcare Products Regulatory Agency (MHRA) - Use of Communications Data**

In January 2011, following a number of illicit importations from India and China of various medicines, a number of addresses were visited by MHRA investigators. It transpired that the addresses were all owned by private mailbox companies and the mailboxes in question were rented by an individual using a fictitious name. However, at one of these companies it was ascertained that an email address had been provided as a contact point for the suspect. A range of subscriber data was acquired in relation to the email address and this identified another mailbox address that was previously unknown to the investigation team. Subsequent enquiries on this mailbox revealed the true identity and home address of the suspect. In June 2011 the address was searched by investigators and £1.6 million pounds worth of unlicensed and prescription only medicines, together with Class C drugs, were found. The suspect was arrested and subsequent computer forensic analysis identified an OCG with potential links to other MHRA investigations. The suspect was charged and pleaded guilty to offences including forgery; possession of false identity documents; conspiracy to supply Class C drugs, and conspiracy to supply prescription only medicines and medicines not on the general sales list. He was sentenced to 44 months imprisonment.

## 7.5.5 Training

The College of Policing (formally the National Policing Improvement Agency) continues to take responsibility for the training and accreditation of police force and LEAs 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 enhance their skill level to the best possible standard.

The College of Policing have now extended their communications data training to applicants, intelligence officers, investigators, analysts, DPs, SPoC Managers and SROs. This will ensure that police forces and LEAs 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.

In my last two annual reports I have commented that 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. Regrettably this is still the case and it is crucial for this gap to be filled to ensure that these public authorities have a good understanding of the procedures.

## 7.5.6 Summary of Communications Data Acquisition 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 and 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 105 individual public authorities were inspected by my inspection team and a further 126 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.

It is evident that public authorities are making good use of communications data as a powerful investigative tool, primarily to prevent and detect crime. It is also apparent that communications data plays a crucial role in the successful outcome of investigations and prosecutions. It is clear that the SPoC system is a robust safeguard to the process.

# 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 National Intelligence Unit (NIU) 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 made under the Prison Act 1952, Function 4 of the National Security Framework (NSF), the Public Protection Manual (PPM), and Prison Service Instructions (PSIs) 49/2011 & 24/2012. 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.

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 in August 2012 as part of PSI 49/2012. 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.

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.

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.

The inspectors also examine the processes relating to the disclosure of material to LEAs to ensure they are fully aligned to the Operational Partnership Team's (formally the Police Advisors Section) 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.

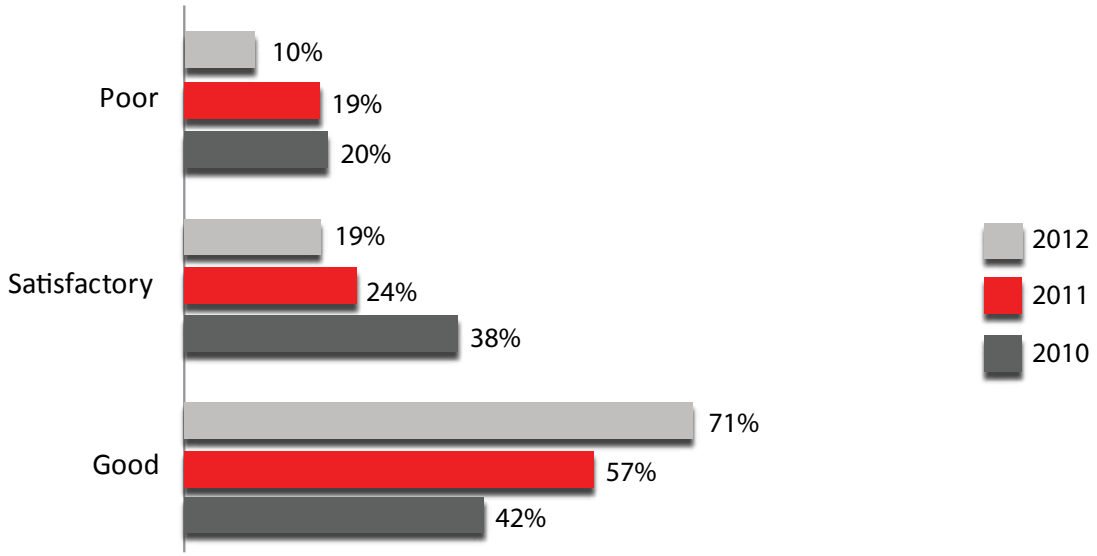
A copy of the report is sent to the Governor or Director of the prison. They are required to confirm, within a prescribed time period, that the recommendations have been achieved or outline the progress they have made against achieving the recommendations. All of the reports are also copied to NIU and the Deputy Director of Custody for the relevant prison region.

## 8.3 Review of 2012 Prison Inspections

At the time of writing this report there are 131 prisons in England & Wales subject to inspections and 3 in Northern Ireland. Since the Inspectorate was formed in 2005 just under 90% of the prisons have been inspected at least four times. During the period covered by this report my inspectors conducted 93 inspections at 92 prisons, which equates to 70% of the whole estate. In addition health checks were also conducted at 2 of the prisons, at the request of the prisons, rather than due to poor compliance.

Figure 20 illustrates that 71% of the prisons inspected achieved a good level of compliance with the Act and Code of Practice. This represents a 14 percentage point increase on the 2011 results which is significant. Although this percentage should be treated with care as the prisons inspected are not the same every year, the prison inspections generally run in two year cycles and therefore it is worthy to note that the 2011 inspections also demonstrated a 15 percentage point improvement on the previous year. In 2012 90% of the prisons achieved either a good or satisfactory level of compliance, in comparison with 81% in the previous year.

**Figure 20 – Comparison of Prison Inspection Results, 2010 to 2012**




These prisons had implemented the majority of their previous recommendations and as a result they had either sustained or 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 a number of the prisons inspected in 2012 and managers and staff clearly demonstrated a commitment to achieve the best possible standards.

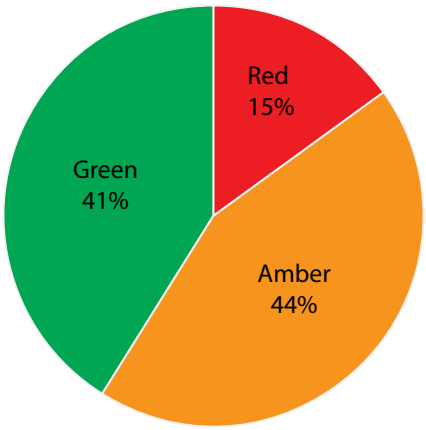
*"71% of the prisons inspected achieved a good level of compliance with the Act and Code of Practice. This represents a 14 percentage point increase on the 2011 results which is significant."*

Last year serious weaknesses and failings were found in the systems and processes of 15 of the prison establishments and this pattern had been fairly static since my first reporting year. In last year's report I outlined that I hoped to report a reduction in the number of poorly performing prisons and therefore this year I am pleased to report that the number of poorly performing prisons has reduced by almost 50 percent. These results are significant and represent a turning point for the prison service.

*"In last year's report I outlined that I hoped to report a reduction in the number of poorly performing prisons and therefore this year I am pleased to report that the number of poorly performing prisons has reduced by almost a half."*

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 545 recommendations were made by my inspectors during the prison inspections and this is an average of 6 recommendations per establishment. Figure 21 shows the breakdown of recommendations by colour.

**Figure 21 – Recommendations from 2012 Prison Inspections**




The percentage of red and amber recommendations has reduced slightly this year to 59%. Although 48 of the prisons inspected received red serious compliance recommendations from their inspections, it is important to make the point that in two thirds of these cases the establishments only received 1 red recommendation. In these establishments the serious non-compliance issues were therefore confined to only one area of the process and a good or satisfactory level of compliance was found in all other areas. This year 8 prisons emerged poorly from their inspections and 45% of the red recommendations emanated from these prisons. Two of these prisons are in Northern Ireland and I have been assured by the Director General of the Northern Ireland Prison Service that the necessary remedial action will be taken. Of the six prisons in England and Wales, five improved markedly on re-inspection in 2012 or early 2013. The remaining one prison has provided an assurance that they will improve their standards, and they will be subject to another re-inspection in 2013.

The red recommendations fitted into three distinct areas; offence related and / or intelligence-led telephone monitoring, record keeping (monitoring logs) and retention periods. Each of these areas will be discussed in the next sections.

First, failings were found in relation to the offence related and / or intelligence-led telephone monitoring procedures in approximately a quarter of the establishments. Last year over half of the prisons inspected were found to have failings in this area, and although I am pleased to report a significant improvement this year, the number of prisons still failing in this area is too high. It is evident that a number of the establishments have worked hard to ensure they have the necessary equipment and resources to conduct the interception properly. Therefore the failures in this area are generally now only seen in prisons where very large numbers of prisoners require monitoring. 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.

*"This is a significant improvement in compliance and is evidence that the establishments have worked hard to ensure they have the necessary equipment and resources to conduct the interception properly"*

Second, my inspectors also found serious failings in relation to the record keeping requirements. Specifically, in some of the establishments there was no evidence that interception had been conducted as monitoring logs had not been completed by the monitoring staff. The majority of these red recommendations related to ad hoc monitoring. In these cases it was recommended that monitoring logs were introduced to ensure that there was a full audit trail of the interception activity. Furthermore in a number of the establishments, amber recommendations were made as although monitoring logs were being completed, there was room to improve their standard of completion. It is important for monitoring logs to be completed to a good standard as these will assist with the review process and provide the Authorising Officer with the information required to decide whether to continue or cease monitoring.

Third, 16% of the prisons were found to be retaining intercept product (generally telephone backup DVDs) for longer than the permitted three month period. This represents a breach of Prison Rule 35D(1). Although this is an improvement on last year (25% failing in this area), it is an area where there is really no excuse for non compliance. 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. One of the prisons that was recently inspected has received the upgrade to the telephone system which eradicates this issue completely as intercept product is automatically destroyed once it reaches three months. Hopefully the rollout of this version will happen in all establishments in 2013.

In a very small number of the prisons inspected, serious failings were identified in relation to the authorisations for monitoring. In two prisons, the authorisations had not been signed by an Authorising Officer of the required grade / level. In addition four of the establishments had failed to take on board the reduced authorisation periods which came into force when the revised NSF was published in February 2009. Offence related monitoring must be reviewed at least every 3 months, and reviews for intelligence-led monitoring must be undertaken within 1 month. As a

result prisoners had continued to be monitored for longer than the permitted period without review. Finally in four prisons monitoring had continued after some of the authorisations had expired due to an administrative error. These were all serious breaches of Prison Rules and / or NSF. Red recommendations were given to these establishments to ensure they align their authorisations to the NSF and introduce robust review processes so that monitoring does not continue if an authorisation has expired.

44% of the recommendations fell into the amber category this year. I can report that there were four areas where amber recommendations were prevalent across a significant number of the prisons; Interception Risk Assessments, reviews, timeliness of the monitoring of prisoners' telephone calls, and record keeping (monitoring logs). Amber recommendations were made in these areas to assist the prisons to tighten their procedures and improve compliance. Each of these areas will be discussed in the following paragraphs with the exception of the record keeping (monitoring logs) which has already been covered earlier in this section.

*"Unfortunately the Prison Service has still not managed to disseminate the new Interception Risk Assessment template that was designed in 2011. I reported last year that the template has been piloted at a number of prisons and I would encourage the Prison Service to introduce this as soon as possible to assist the prisons to achieve a better level of compliance in this area."*

My inspectors were pleased to find that the vast majority of the prisons were completing Interception Risk Assessments for prisoners who meet the criteria for offence related monitoring; however my inspectors concluded they were not completed to a satisfactory standard in a third of the establishments inspected. A number of the question sets had not been properly completed and as a result there was a lack of information in relation to the factors that had been taken into account and risk assessed. With the lack of evidence in the risk assessments, it was difficult to see how the Authorising Officers were able to make informed decisions as to whether monitoring was necessary and proportionate. In addition my inspectors concluded that in a quarter of the establishments inspected, the reviews for the monitoring authorisations (offence related and / or intelligence-led) did not adequately set out the reasons why it was deemed necessary to continue or cease monitoring. Recommendations were made in these two areas to ensure that the risk assessments and any authorisation reviews contain sufficient evidence to support the Authorising Officers decisions to initiate, continue or cease monitoring. Unfortunately the Prison Service has still not managed to disseminate the new Interception Risk Assessment template that was designed in 2011. I reported last year that the template has been piloted at a number of prisons and I would encourage the Prison Service to introduce this as soon as possible to assist the prisons to achieve a better level of compliance in this area.

Finally, my inspectors identified that a number of the prisons were not listening to the offence related or intelligence-led calls in a timely fashion or within the timescale outlined in the authorisations. It is vitally important for the prisons to ensure that all calls made by prisoners subject to offence related or intelligence-led monitoring are listened to within a timely fashion in order to evaluate the risk or threat these prisoners pose.

This year 41% of the recommendations were green. These recommendations were not compliance issues and were generally made to assist the prisons to improve the efficiency and effectiveness of their interception processes.

## 8.4 Summary

In the reporting year 93 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.

I am pleased to report that the percentage of poor performing prisons has reduced by almost 50 percent this year. I am also encouraged by the fact that a large number of the prisons have clearly improved their level of compliance.

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. 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. 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.

# 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 interception of communications or acquisition of communications data, how I conduct my oversight role and, to the extent possible, my assessments of compliance at the public authorities I oversee.

## 9.1 Opening Address to the International Communications Data & Digital Forensics Conference

I was invited to give a speech at the International Communications Data & Digital Forensics Conference in March 2012. The conference was organised by the ACPO Data Communications Group. The delegates at the conference were mainly LEA staff (investigators, analysts, digital forensic staff, Senior Investigating Officers, SPoCs, DPs and SROs) and staff from various CSPs. There were also a number of representatives from foreign LEAs and private companies involved in forensic communications. The conference is made up of a large number of seminars covering various communications data and digital forensic inputs. Delegates can decide which seminars to attend in order to further their technical knowledge.

My speech focused on Part I Chapter 2 of RIPA and I welcomed the opportunity to explain how I saw my role as Interception of Communications Commissioner and that of my inspectors. My speech covered the importance of communications data to terrorist and crime investigations, the importance of ensuring that staff in this field are adequately trained and the need to ensure that the capability to acquire data is maintained. I discussed the continuing threats, challenges and opportunities of the technological advancements, my function in relation to the oversight of errors and the responsibility of all involved in the process to provide the public with the necessary reassurance that public authorities are using their powers lawfully, responsibly and effectively.

## 9.2 Meeting with Intelligence and Security Committee

In April 2012 the Intelligence Services Commissioner, 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 and Security 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, the role of NAFN in relation to local authority access to communications data and the proposals for intelligence oversight reform.

## 9.3 Oral and Written Evidence to the Communications Data Bill Joint Select Committee

I provided written evidence to the Joint Committee appointed to conduct the pre-legislative scrutiny of the draft Communications Data Bill and I also provided the Committee with copies of my 2011 Annual Report. My written evidence can be accessed at the following link http://www.parliament.uk/draft-communications-bill/ I was invited to give oral evidence, with my Chief Inspector, to the Joint Committee on 16th October 2012. This oral evidence session can be watched via the following link http://www.parliamentlive.tv/Main/MeetingDetails.aspx?meetingId=11518.

I do not intend to outline my written and oral evidence in full here, but I will comment on the key areas of the bill that impact on my role and respond to some of the Committee's recommendations. Broadly I am satisfied that the legislation is required in order to ensure that public authorities have a continuing capability to obtain communications data in the future.

I am pleased that the draft bill does not change the current application or authorisation process for the acquisition of communications data. Requests will only be made by the public authorities approved by Parliament to acquire data and the requests will be vetted by a SPoC and approved by a designated senior officer who must believe the tests of necessity and proportionality have been met. I have long been a proponent for the SPoC process and believe it is a robust safeguard.

The new powers will also provide for filtering arrangements, which will minimise the amount of communications data that is disclosed to a public authority when more complicated data requests are made, thus minimising the intrusion into privacy. The Interception of Communications Commissioner will have the responsibility to oversee the filter and I was assured by senior Home Office staff that my successor would be provided with the necessary resources to carry out this new function and would be consulted in relation to the design, testing and implementation of any filter. This is crucial to ensure effective oversight of the filter.

In addition the draft bill will close the loophole through which local authorities and some other public authorities are able to use other powers (such as the Social Security and Fraud Act 2001) to acquire communications data. I welcome this and have expressed concerns in the past that two regimes exist for acquiring communications data in some public authorities. The current RIPA process (to be replaced by the CD bill) is a robust system. The process is subject to oversight and the means of redress for complaints is through the Investigatory Powers Tribunal. Other pieces of legislation that are currently used to acquire communications data do not have any such oversight and the authorisation levels are typically set to a lower level. The draft bill proposes to remove these other statutory powers with weaker safeguards.

I strongly believe that the powers should not be limited to just police forces and intelligence agencies. Parliament has delegated statutory enforcement functions to a number of other public authorities and as a result they have a clear statutory duty to investigate a number of criminal offences, some of which are their sole responsibility. Often the criminal offences that these public authorities investigate are regarded as very important at a local level and provide the public with reassurance and protection. I have given a number of examples of such investigations in this report. The volume of requests is low, but this does not mean that such public authorities should

not be able to use the powers when they can demonstrate it is necessary and proportionate to do so. It is sensible for the Government to take the opportunity to review the current list of public authorities who have access to ensure that access is still required, but that review should keep in mind the need to have powers available when they can properly be used.

The Joint Committee published their report in December 2012 and made a number of recommendations. I strongly agree with the Committee's recommendation in relation to removing the magistrate process for local authorities if a "super SPoC" is used and this will be covered in the next section of my report. The NAFN SPoC service has been a great success for local authorities and I agree that it would also be a good idea to require other infrequent users of communications data to follow this model.

The Committee concluded that public confidence may be built by making the communications data inspections conducted by my office more thorough and the inspection reports more detailed. I am satisfied that the inspections conducted by my office are thorough and I have attempted to provide more information in my annual report this year to evidence this. Furthermore I am satisfied that our inspection reports are already detailed. A number of public authorities have openly published their inspection reports in line with the provision in the Code of Practice.

The Committee recommended that my office should carry out a full review of each of the large users of communications data every year and outlined that they would prefer to be reassured that in the case of every authority submitting fewer than 100 applications a year they were all routinely examined. No doubt my successor will make a decision on the frequency of the inspections of larger users. I have taken a preliminary look at the figures from the inspections and ascertained that in almost all instances where fewer than 100 applications a year were submitted, my inspectors examined every one.

The Committee recommended that my annual report should include more detail; including statistics, about the performance of each public authority and the criteria against which judgments are made about performance. It should analyse how many communications data requests are made for each permitted purpose. I have long recognised the limitation of the current statistics that public authorities are required to retain and report (as stipulated by the Code of Practice). For a number of years my office has wanted to increase the record keeping requirements in this respect, but this requires a change to the Code of Practice. The current statistics are incomplete as it is not possible to discern the number of individual items of data requested. The proposed legislation would be an opportunity to address this.

The Committee also recommended that my brief should explicitly cover the need to provide advice and guidance on proportionality and necessity, and there should be rigorous testing of, and reporting on, the proportionality and necessity of requests made. I can advise that my inspectors have always provided advice and guidance on these principles to assist public authorities to meet the requirements. What's more, the principles are rigorously tested during the inspections and this year I have provided some examples in my annual report of where my inspectors challenged the necessity and / or proportionality justifications for acquiring the data.

I am pleased that the Committee thought my view that the system is broadly working well, that comparatively few errors are made, that only a few of these are serious, and that my inspectors do a thorough job through which they can discover where the system is failing, and make recommendations to put this right which are followed, was a fair summary.

## 9.4 Protection of Freedoms Act 2012 (Judicial Approvals for Local Authority Communications Data Requests)

I have previously reported that I was unconvinced that the Government's proposal to require all local authorities to obtain judicial approval before they can acquire communications data would lead to improved standards or have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data. The Protection of Freedoms Act 2012 came into force in this respect on 1st November 2012 and regrettably the evidence that has been shared with my office to date reinforces my standpoint.

I can report that NAFN have seen a 63% reduction in the number of applications submitted by local authorities in the first four months of the legislation being enacted. I do not believe that local authorities have stopped requesting the data because they no longer need it, but I suspect the reason they have stopped is due to the overly bureaucratic and costly process now in place.

Local authorities have reported experiencing lengthy time delays in just obtaining an appointment with a magistrate (in the worst case 6 weeks). Other local authorities have reported that the magistrates were totally unaware of the legislation and as a result they had to provide them with advice and guidance. This is worrying, particularly considering the Home Office gave a commitment to properly train the magistrates to carry out this role. In one case that has been reported to my office, the magistrate did not ask to see the application form which set out the necessity and proportionality justifications, or the DPs approval. The application was approved on the basis of a verbal briefing from the applicant and DP. It is extremely concerning that the paperwork in this case was not examined to check that it had been properly authorised. Furthermore, in this case the local authority failed to serve the judicial application / order form on the CSP with the associated Section 22(4) Notice, but the CSP disclosed the data without question. There was no evidence that the acquisition of the data has been lawfully approved in the absence of the judicial application / order form and therefore it is worrying that the CSP disclosed the data in this case.

I was informed by the Home Office that Her Majesty's Court Service (HMCS), which falls under the remit of the Ministry of Justice, concluded that it would not be possible to manage the judicial process electronically. This is regrettable and has meant that the judicial part of the process has had to be dealt with manually outside of the fully electronic, auditable application system that is in place at NAFN. This significantly increases the administrative burden. There is also the possibility of more errors occurring as the communications addresses have to be double keyed. Furthermore I have also been informed by the Home Office that HMCS did not think that it would be possible for the judicial part of the process to be managed by the NAFN SPoCs attending their local courts in the Tameside and Brighton areas, as it would place too much burden on those courts. As a result each application gets bounced back and forth between the applicant in the local authority, the SPoC at NAFN, the DP in the local authority and the

magistrate in the local court, which increases bureaucracy and time delays. Often the applicant is not best placed to advise the magistrate on the communications data process or the conduct that will be undertaken by the SPoC to acquire the data. In other cases, local authorities have actually reported that the courts have tried to charge them directly for attending the court. The figures that have been shared with my office to date show that no requests have yet been refused by a magistrate.

Taking into account this evidence I question how much value judicial approvals have added to the process. I have long been a proponent of the SPoC system and this ensures there is a robust safeguard in relation to the acquisition and disclosure of communications data. The Joint Committee conducting the pre-legislative scrutiny of the draft Communications Data Bill concluded that *"in the case of local authorities it should be possible for magistrates to cope with the volume of work involved in approving applications for authorisation. But we believe that if our recommendations are accepted and incorporated into the Bill, they will provide a stronger authorisation test than magistrates can. Although approval by magistrates of local authority authorisations is a very recent change in the law, we think that if our recommendations are implemented it will be unnecessary to continue with different arrangements applying only to local authorities."* I concur with this sentiment and am very concerned that there is a serious danger that that the types of crime that cause real harm to the public (such as rogue traders and illegal money lenders) will not be investigated properly due to the difficulties with the judicial approval process.

## 9.5 Data Protection Forum

I accepted an invitation in December 2012 to attend the Data Protection Forum and had the opportunity to informally discuss 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.

## 9.6 International Delegations

In May 2012 I attended the International Intelligence Review Agencies Conference in Ottawa, Canada. This is an opportunity to meet with other national review organisations from around the world and to discuss our roles, responsibilities and oversight regimes. At the conference I gave a presentation jointly with the Rt Hon. Sir Malcolm Rifkind MP, Chairman of the Intelligence and Security Committee.

## 9.7 Meeting with Other Oversight Commissioners

In November 2012, with my successor Sir Anthony May, I met with some of the other Commissioners involved with intelligence, security and/or data oversight where we discussed matters of common interest.

# 10. CONCLUSION

This is my final report as Interception of Communications Commissioner covering the period between 1st January and 31st December 2012. I stood down as Interception of Communications Commissioner at the end of this period and am not in a position to deal with events after that period.

I believe that it is in the public interest that public authorities should demonstrate that they make lawful, responsible and effective use of their powers. My annual report should provide the necessary assurance that the use which public authorities and prisons have made of their powers under RIPA and Prison Rules respectively has met my expectations and those of my inspectors, and that I have reported on the small number of occasions where it has not. I have increased the level of detail in my annual reports each year to enable the public to have a better understanding of what is overseen, how it is overseen, and the impact of independent oversight.

The use of lawful interception and communications data affords significant advantages to public authorities when investigating crime and threats to national security. Although huge intelligence and investigative benefits can be reaped from lawful interception and communications data, interception and the gathering of data has the potential to be highly intrusive. That is why the tests of necessity and proportionality outlined in RIPA and the independent scrutiny provided by my team and others tasked with intelligence oversight are crucial.

It is my view, based on the results from the inspections that my inspectors' and I have conducted, that the public authorities and prisons which I oversee strive to achieve the best possible level of compliance with RIPA and Prison Rules respectively.

I have observed, both this year and during previous years that questions concerning the legality and the necessity and proportionality of the proposed conduct are posed at every stage of the application and authorisation process. Through my reading of documents and my meetings with staff involved in interception and the acquisition of communications data, I have been able to reach the conclusion that all those involved act with integrity and in an ethical manner. The greatest scrutiny occurs within the public authorities themselves. For example, in relation to lawful interception, an application 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 relevant Secretary of State. I have observed that successive ministers of different political persuasions, senior officials, public authority and CSP staff have all undertaken this internal scrutiny with dedication and integrity. Similar safeguards exist in relation to the acquisition of communications data, where the requests are vetted by a trained and accredited SPoC before being considered by a DP, who must believe the tests of necessity and proportionality have been met. I have long been a proponent for the SPoC process and believe it is a robust safeguard to the communications data process.

Error reporting remains a significant component of my oversight function. It is perhaps inevitable that some mistakes will be made, especially when public authorities are dealing with large volumes of interception product and communications data in complex investigations. However, I am pleased to say that the error rate is very low when compared to the volume of communications data requests made and interception warrants in place. I am confident that errors are generally reported on time, in full and that steps are taken to reduce the likelihood of

such errors recurring. My inspectors and I also investigate the circumstances of any errors and work with the public authorities and CSPs concerned to review their systems and processes where necessary. I am satisfied that when issues of compliance arise during inspections these are promptly corrected and I am impressed with the dedication and willingness of staff to implement any recommendations arising from their inspections.

As I said at the beginning of this report, much has changed in the world of communications since I began as Commissioner in 2006. The technology continues to evolve, and sophisticated criminals and terrorists are quick to make use of the latest developments, so those who seek to prevent acts of terrorism and to investigate serious crime need to have the resources they require to be effective. They should not be hampered by legislation enacted at a time when much of what is now taken for granted had not even been heard of. As a nation we have enormous advantages, including in particular the integrity of those who work in our security services and law enforcement agencies, and we need to listen to them, especially when they say that changes need to be made to try to retain our present capacity. That is not to say that RIPA is completely out of date. In many ways it has weathered well, and the system of oversight which it laid down has been, I believe, effective, but if changes need to be made in order to retain capacity they should not be resisted. I also believe that it is important for independent oversight to remain as a key component of any future legislation.

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


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 Houses of Parliament Shop
12 Bridge Street, Parliament
Square, London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

**TSO@Blackwell and other accredited agents**

ISBN 978-0-10-298659-4

9 780102 986594

HO_01939_G