2013 Annual Report of the Interception of Communications Commissioner

The Rt Hon.
Sir Anthony May

2013 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 8th April 2014

Laid before the Scottish Parliament by the Scottish Ministers 8th April 2014

HC 1184

SG/2014/25

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to: info@iocco-uk.info

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

Print ISBN 9781474101578

Web ISBN 9781474101585

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID 2633623 04/14

Printed on paper containing 75% recycled fibre content minimum

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

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

April 2014

Dear Prime Minister,

You appointed me under Section 57(1) of the Regulation of Investigatory Powers Act (RIPA) 2000 as Interception of Communications Commissioner to take office from 1st January 2013 upon the retirement of the Rt Hon. Sir Paul Kennedy, who had held the office for six years. I am required by Section 58(4) of RIPA to make a report to you with respect to the carrying out of my statutory functions as soon as practical after the end of each calendar year. This is my first annual report covering the calendar year 2013.

You are required to lay a copy of my annual report before each House of Parliament (Section 58(6)) together with a statement as to whether any matter has been excluded from that copy because it has appeared to you after consulting me, that publication of that matter would be contrary to the public interest or prejudicial to matters specified in Section 58(7) of RIPA. For reasons which I discuss briefly in the body of this report, there is no suggested Confidential Annex or matters to be excluded from publication. You may, of course, decide otherwise, but my expectation is that you will feel able to lay this entire report before parliament.

Yours sincerely,

The Rt Hon. Sir Anthony May
Interception of Communications Commissioner

Contents

Section 1
Introduction

1.1 This report is rather differently presented, both in its form and some of its content, from recent reports of my predecessors.

1.2 My first aim is to fulfil my statutory obligation for 2013 to report annually to the Prime Minister. My second aim is to address, so far as I am able in a report to be laid before Parliament, public concerns relevant to my statutory function raised by media publications based on disclosures reportedly made during 2013 as a result of Edward Snowden's actions.

1.3 Some of these disclosures have related to alleged interception activities of UK intelligence agencies. They have suggested that these agencies have, or may have, misused their interception powers or capabilities. It was plain that I should investigate these suggestions thoroughly, which I now have.

1.4 Public concern has centred on potential intrusive invasion of privacy. Such concern has been expressed publicly in the United States, Europe and other countries with greater force perhaps than in the UK. But unjustified and disproportionate invasion of privacy by a public authority in the UK would breach Article 8 of the European Convention on Human Rights just as much here as in other parts of the European Union.

1.5 Concerns of this kind are legitimately raised and need to be addressed. They derive to a significant extent from a lack of detailed understanding of the legislation which enables lawful interception of communications to take place; and a lack of information about what the interception agencies actually do or, just as importantly, what they do not do.

1.6 I have very considerable sympathy with those who are hazy about the details of the legislation. The Regulation of Investigatory Powers Act 2000 (RIPA 2000) is a difficult statute to understand. An important change of presentation in this report is that I shall give a narrative outline of the relevant statutory provisions in what I hope will be a reasonably accessible form with an eye to the disclosures. Because RIPA 2000 Part I is difficult legislation, this narrative may in places be dense and perhaps itself indigestible. I have tried to make it as accessible as possible, but apologise if I have not entirely achieved this.

1.7 It is not so easy to give a relevant public account of what the interception agencies actually do because much of it is sensitive. In this report, I am constrained by statutory provisions forbidding disclosure. But an important change of presentation in this report is that I shall try to be more informative than my predecessors felt they needed to be. To this end, I am not submitting any suggested Confidential Annex to this report to the Prime Minister[1]. I do not consider that a confidential annex is presently necessary. That does not mean that one may not be needed in the future.

1.8 I have included at the end of each of the main Sections of the report "Points of Note" which summarise highlights of the contents of those Sections.

1 It is strictly for the Prime Minister to decide which parts of this report should be made public by laying them before Parliament – see section 58(7) of RIPA 2000.

Section 2
My Role

2.1 I was appointed as Commissioner in January 2013. It necessarily took me some time to become familiar with the details of RIPA 2000 Part I and its Codes of Practice and with the procedures which these require. I also needed to get to grips with the various technical operations and systems which the public authorities undertake or use. I ventured conversationally at the outset that this familiarisation and education process might take me up to a year. In the round, so it has proved.


The Rt Hon. Sir Anthony May

2.2 My principal powers and duties are in section 57(2) of RIPA 2000. They relate mainly to RIPA 2000 Part I (sections 1 to 25).

RIPA Part I

2.3 RIPA 2000 Part I divides into two Chapters.

- Chapter I (sections 1 to 20) concerns the interception of the content of communications and the obtaining of related communications data.
- Chapter II (sections 21 to 25) concerns the acquisition and disclosure of communications data. Communications data do not embrace the content of the communication.

Interception of content

2.4 Section 1(1) of RIPA 2000 makes it an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public postal service or public telecommunication system. My statutory role concerns interception within the United Kingdom.

2.5 **Interception Warrants.** The main source of lawful authority to intercept the content of a communication is a warrant issued by a Secretary of State under section 5 of RIPA 2000[2]. There are detailed requirements for these warrants. There are also detailed restrictions and safeguards on the use that may lawfully be made of the product of lawful interception of communications. Importantly, section 15(3) requires the destruction of intercepted material and any related communications data (as defined in section 20) as soon as there are no longer any grounds for retaining it as necessary for any of the purposes authorised in section 15, which embrace the statutory purposes in section 5(3).

2 See section 1(5) of RIPA 2000 for other sources of lawful authority.

2.6 The requirements of Part I Chapter I are supplemented in detail by a Code of Practice *"Interception of Communications"* laid before both Houses of Parliament by the Secretary of State and approved by a resolution of each House (sections 71(1), (4), (5) and (9)).

Communications data

2.7 The structured procedure required by Part I Chapter II for the acquisition and disclosure of communications data is different. Here essentially the statutory authority has to be an authorisation granted or requirement made by a senior designated person (DP) in the relevant public authority, who should normally be independent of the investigation to which the application relates (sections 22(3), (4)).

2.8 The provisions of Part I Chapter II are supplemented by a detailed Code of Practice *"Acquisition and Disclosure of Communications Data"* again laid before Parliament and approved by resolution under section 71.

My main powers and duties

2.9 These are under section 57(2) and relate to RIPA 2000 Part I. They are to keep under review;

- the exercise and performance of the Secretary of State of the powers and duties in sections 1 to 11, that is those relating to the granting and operation of interception warrants;
- the exercise and performance by the persons on whom they are conferred or imposed of the powers and duties under Part I Chapter II, that is those relating to the acquisition and disclosure of communications data; and
- the adequacy of arrangements for safeguards relating to use that is made of interception material under section 15, which also embraces additional safeguards in section 16.

2.10 In short, I am required to audit the interception of the content of communications and the acquisition and disclosure of communications data under RIPA 2000 Part I. I am not involved with matters which are the responsibility of the Intelligence Services Commissioner (The Rt Hon. Sir Mark Waller) or the Chief Surveillance Commissioner (The Rt Hon. Sir Christopher Rose).

Reporting to the Prime Minister

2.11 I regard my principal function as being to satisfy myself, and thus to report to the Prime Minister, that the Secretaries of State and the public authorities operating under RIPA 2000 Part I do so lawfully and in accordance with the statute.

2.12 I am required by section 58(2) to report to the Prime Minister contraventions of the provisions of the Act in relation to any matter with which I am concerned that has not been the subject of a report made to the Prime Minister by the Investigatory Powers Tribunal (IPT). I am not aware of any such report by the IPT which bears on my responsibilities. The Errors Sections of this Report (see Paragraphs 3.58 to 3.68 & 4.45 to 4.54) constitute a principal part of the performance of the requirements of section 58(2).

2.13 My principal statutory responsibility is to review the lawfulness of RIPA 2000 Part I activities under existing legislation. I do not regard myself as a practical promoter of legislation. Change and matters of policy are for others, Parliament in particular, to consider and decide. On the other hand, I am better informed than most people outside the public authorities themselves about the way in which RIPA 2000 Part I activities are conducted both in principle and in detail. Addressing, as I shall attempt to do, some of the issues which are of public concern can only be done if I touch on some matters of policy.

Disclosure to the Commissioner

2.14 Section 58(1) of RIPA 2000 imposes a statutory obligation on everyone concerned with the lawful interception of communications and the acquisition and disclosure of communications data under RIPA 2000 Part I to disclose or provide to me all such documents or information as I may require for the purpose of enabling me to carry out my functions under section 57. I have found that everyone does this without inhibition. I am thus fully informed, or able to make myself fully informed, about all the interception and communications data activities to which RIPA 2000 Part I relates however sensitive these may be.

Prisons

2.15 My functions also by convention include the oversight of the interception of prisoners' communications within prisons. This is lawful interception under section 47 of the Prison Act 1952, section 39 of the Prisons (Scotland) Act 1989 and section 13 of the Prison Act (Northern Ireland) 1953 (prison rules) – see section 4(4) of RIPA 2000. My oversight of interception in prisons in England, Wales and Northern Ireland (but not at the moment Scotland) is by non-statutory agreement between the prison authorities and my predecessors.

Section 3
Interception of Communications

3.1 In this section I shall provide an outline of the interception legislation, give details in relation to our interception inspection regime and outline the key findings from our inspections.

Applications for Interception Warrants

3.2 The main mechanism by which interception of communications may be lawful under RIPA 2000 Part I requires the Secretary of State to issue an interception warrant under section 5(1). The conduct authorised by an interception warrant includes conduct to obtain the content of the communication and also conduct to obtain related communications data (as defined in section 20 and Part I Chapter II).

3.3 **Applicant.** An application for an interception warrant cannot be issued except on an application made by or on behalf of the persons listed in section 6(2) of RIPA 2000. Those persons are;

- the Director General of the Security Service (Mi5),
- the Chief of the Secret Intelligence Service (Mi6),
- the Director of the Government Communications Headquarters (GCHQ),
- the Director General of the National Crime Agency,
- the Commissioner of the Metropolitan Police,
- the Chief Constable of the Police Service of Northern Ireland (PSNI),
- the Chief Constable of Police Scotland,
- the Commissioners of Her Majesty's Revenue and Customs (HMRC),
- the Chief of Defence Intelligence, Ministry of Defence.

3.4 **Secretaries of State.** Interception warrants have to be authorised personally by a Secretary of State (section 5(1) and 7(1)(a)). The Secretary of State has to sign the warrant personally, except in an urgent case where the Secretary of State has authorised the issue of a warrant which is then signed by a senior official (section 7(1)(b)).

3.5 There are in practice four Secretaries of State and one Scottish Minister who undertake the main burden of authorising (or declining) interception warrants. The Secretaries of State and Minister mainly concerned are;

- the Foreign Secretary;
- the Home Secretary;
- the Secretary of State for Northern Ireland;
- the Defence Secretary; and
- the Cabinet Secretary for Justice for Scotland[3].

3 Interception warrants may be issued on "serious crime" grounds by Scottish Ministers, by virtue of arrangements under the Scotland Act 1998. In this report references to the "Secretary of State" should be read as including Scottish Ministers where appropriate. The functions of the Scottish Ministers also cover renewal and cancellation arrangements.

3.6 Each of the Secretaries of State have senior officials and staff. Their functions include scrutinising warrant applications for their form, content and sufficiency, and presenting them to the relevant Secretary of State with appropriate suggestions.

3.7 **Statutory necessity purposes.** The Secretary of State is forbidden from issuing an interception warrant unless he or she believes that it is *necessary*:

- in the interests of national security;
- for the purpose of preventing or detecting *serious* crime;
- for the purpose of safeguarding the economic wellbeing of the United Kingdom (which has to be directly related to state security).[4]
- for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a serious crime warrant to give effect to the provisions of any international mutual assistance agreement (section 5(3)).

3.8 These statutory purposes and the requirement of necessity come directly from Article 8 of the Human Rights Convention. To issue an interception warrant for any other purpose would be unlawful. Needless to say, Secretaries of State do not issue interception warrants for other purposes. It is part of my function to make sure that they do not.

3.9 **Proportionality.** The Secretary of State is forbidden from issuing an interception warrant unless he or she believes that the conduct authorised by the warrant is *proportionate* to what is sought to be achieved by that conduct.

3.10 Proportionality pervades human rights jurisprudence and is explicitly central to the lawful operation of RIPA 2000. Every application for a Part I Chapter I interception warrant has to address proportionality explicitly. Secretaries of State have to address proportionality in the judgment they apply to decide whether or not to issue an interception warrant. A judgment whether it is proportionate to issue the interception warrant requires holding a balance between (a) the necessity to engage in potentially intrusive conduct and (b) the anticipated amount and degree of intrusion. The judgment has to consider whether the information which is sought could reasonably be obtained by other less intrusive means. This is explicit for interception (section 5(4)). Warrants are refused (or never applied for) where it is judged that the necessity does not outweigh the intrusion.

3.11 **Types of Interception Warrants.** There are essentially two types of interception warrants. Section 8(1) warrants and section 8(4) warrants.

3.12 All interception warrants are for the interception of the content of communications

---

4 See Directive 97/66/EC.

and related communications data.

3.13 All interception warrants may comprise communications not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises (section 5(6)). These are communications which you cannot technically avoid intercepting if you are going to intercept the communications which the warrant expressly authorises.

3.14 All applications for warrants have to be in writing and usually cover several pages. The Secretaries of State have available to them in the applications detailed supporting information including specific sections directed to the protection of privacy.

3.15 Interception warrants have an initial duration of *6 months* where the statutory purpose is national security or economic wellbeing of the United Kingdom, but *3 months* where the statutory purpose is serious crime (section 9(6)). They cease to have effect at the end of the period unless they are renewed.

3.16 An interception warrant may be renewed at the end of the relevant period by the Secretary of State personally, but only if the Secretary of State believes that it continues to be necessary for a statutory purpose (section 9(2) and paragraphs 4.13 and 4.14 of the Code of Practice). Applications for renewals have to contain details justifying the necessity for renewal giving an assessment of the intelligence value of the interception to date.

3.17 The Secretary of State is required to cancel an interception warrant if he or she is satisfied that it is no longer necessary for the authorised purpose (section 9(3) and paragraph 4.16 of the Code of Practice). This in practice means that the interception agency should apply for cancellation of a warrant that is no longer necessary.

3.18 Exceptionally a warrant may be issued in an urgent case by a senior official if it is expressly authorised by a Secretary of State (section 7(1)(b), 7(2)(a) and paragraph 4.6 of the Code of Practice). An urgent warrant lasts for 5 days unless it is renewed by the Secretary of State (section 9(6)(a)).

3.19 **Section 8(1) interception warrants** must name or describe either (a) one person as the interception subject, or (b) a single set of premises as the premises to which the permitted interception relates (section 8(1) itself). The definition of "person" in section 81(1) includes any organisation or any association or combination of persons, but that does not detract from the individuality of the required warrant definition.

3.20 A section 8(1) warrant should contain the details required by paragraph 4.2 of the Code of Practice. The required details include:

- the background of the operation,
- the relevant person or premises the subject of the application;
- the communications to be intercepted;

- an explanation of the necessity for the interception;
- a consideration of why the conduct is proportionate;
- consideration of any unusual degree of collateral intrusion, not least if the communications might be privileged; and
- an assurance that all intercepted material will be handled in accordance with the safeguards in section 15 of RIPA 2000.

3.21 Section 8(1) warrants have to comprise one or more schedules with details designed to tell the relevant communication service provider (CSP) which communications they are required to intercept (section 8(2)).

3.22 **Section 8(4) interception warrants.** Section 8(4) disapplies the provisions of section 8(1) and 8(2) in certain circumstances. This means that a section 8(4) warrant does not have to name or describe one person as the interception subject or a single set of premises as the target of the interception.

3.23 Section 8(4) warrants are restricted to the interception of external communications. External communications are communications sent or received outside of the British Islands (see section 20).

3.24 Section 8(4) warrants should contain the details required by paragraph 5.2 of the Code of Practice. I have for convenience described the statutory structure for section 8(4) warrants in further detail in Section 6 (Question 5) of this report to which I refer the reader.

3.25 **Safeguards.** These apply to both types of interception warrants. Section 15(2) strictly controls the dissemination of intercepted material. The section requires that dissemination of intercepted material is limited to the minimum necessary for the authorised purposes. All material (including related communications data) intercepted under section 8(1) or 8(4) must be handled in accordance with safeguards which the Secretary of State has approved under the duty imposed by RIPA 2000.

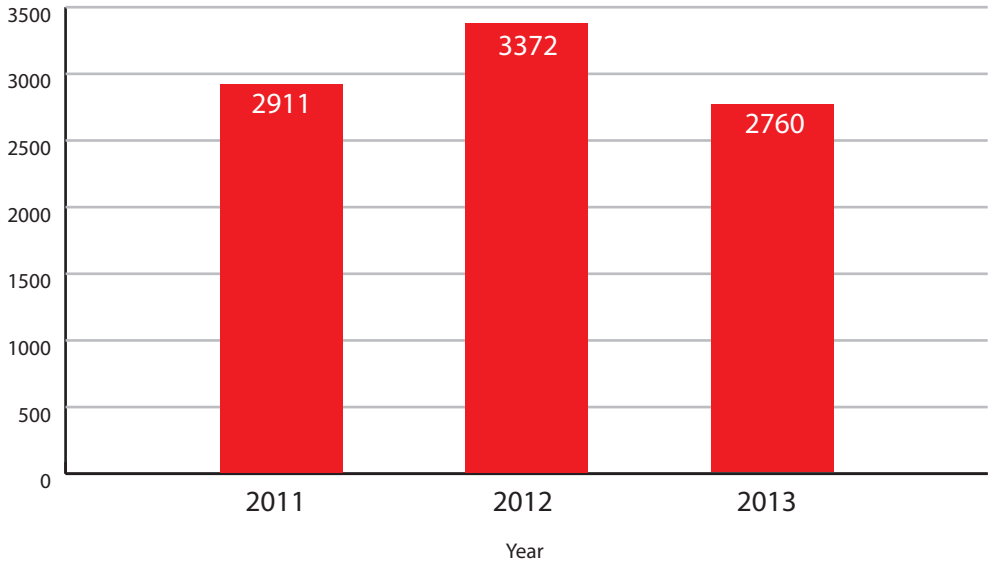
3.26 Section 15(3) requires that each copy of intercepted material and any related communications data is destroyed as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes.

3.27 There are additional safeguards for Section 8(4) warrants and these are described in Section 6 (Question 5) of this report.

Statistics for Interception Warrants

3.28 Figure 1 shows the number of interception warrants authorised in each of the years 2011 - 2013 for the 9 relevant interception agencies. The total number of interception warrants authorised during the calendar year 2013 was 2760. This is a reduction of 19%

Figure 1 *Total Number of Interception Warrants Authorised 2011-13*



on 2012. The total number of warrants extant on 31 December 2013 was 1669. These numbers generally show, as is the fact, that numerous warrants do not run for longer than a number of months.

Inspection Regime

3.29 **Objectives of Inspections.** The primary objectives of our inspections are to ensure:

- that the systems in place for the interception of communications are sufficient for the purposes of the Part I Chapter I and that all relevant records have been kept;
- that all interception has been carried out lawfully and in accordance with Part I Chapter I and its associated Code of Practice; and,
- that any "errors" are reported to me and that the systems are reviewed and adapted where any weaknesses or faults are exposed.

3.30 **Number of Inspections**. I have since I was appointed personally undertaken a full programme of interception agency inspections. I have inspected each of the 9 interception agencies authorised to apply for interception warrants at approximately six monthly intervals, that is twice each during 2013.

3.31 The first series of inspections was in the Spring and early Summer. They mainly followed the pattern established by Sir Paul Kennedy, my predecessor, as described in his

2012 Report. They enabled me to become more familiar with the requirements of my statutory role.

3.32 The second series of inspections was in the Autumn and Winter of 2013. For these, we made some significant changes in our procedures as follows:

- we increased the inspection time spent with each interception agency. Most of the inspections ran over two days, the first of which we generally used for reading warrantry and other documents in preparation for the second day's investigations. These investigations covered those selected operations or warrants which required further explanation;
- we carried out or continued a full investigation where necessary into matters raised by media disclosures;
- we instigated a thorough investigation of the arrangements in place for the Retention, Storage and Destruction of intercepted material and related communications data. (See paragraphs 3.48 to 3.57 for further detail);
- we instituted what will now become our standard procedure of producing a detailed written report and recommendations from each inspection. This is sent to the Head of the relevant interception agency with a copy for the relevant Secretary of State.

3.33 I also inspected the work of the senior officials and staff in the relevant parts of the main Secretary of State departments at six monthly intervals. The officials provide good support and advice to the Secretaries of State and are a channel of communication and advice with the interception agencies. I visited the main warrant issuing Secretaries of State at the end of the 2013 or early in 2014.

3.34 In addition to 26 interception inspections conducted in 2013, I also visited the interception agencies on a number of occasions to follow up points arising from our inspections or on other matters.

3.35 Examination of warrants. We inspect the systems in place for applying for and issuing interception warrants under sections 8(1) and 8(4). We scrutinise what I regard as a representative sample (chosen by me) of the warrantry paperwork. In this context warrantry paperwork includes warrant applications, renewals, modifications, cancellations and their associated instruments and schedules. Much of this is on paper, but in some interception agencies we now have access to and personally interrogate the computer systems that the agencies use. This enables us to audit the process from start to end and to examine the product gained from the interception.

3.36 Samples. The total number of warrant applications specifically inspected during the 26 interception inspections was approximately 600. The associated warrantry paperwork in relation to these applications was also examined. This represents just over one third of the number extant at the end of the year and one fifth of the total of new warrants issued during the year.

3.37 It is important that we scrutinise a sufficient representative sample of the individual warrants. The representative sample includes appropriate selections from various crime types and national security threats. But, in my view, inspecting and understanding systems is in the end as important as scrutinising yet more individual warrant applications.

3.38 **Inspection Reports.** The reports contain formal recommendations with a requirement for the interception agency to report back to me within two months to say that the recommendations have been implemented, or what progress has been made. These are sensitive documents, but, speaking generally, they contain:

- an account of the inspection, including a list of the particular warrants inspected;
- assessments of the interception agency's compliance with statutory requirements;
- an account of the errors reported by the interception agency to my office during the inspection period; and
- a number of structural recommendations aimed at improving the interception agency's compliance and performance generally.

Inspection Findings and Recommendations.

3.39 My inspections demonstrate that the paperwork is almost always compliant and of a high quality. If there are occasional technical lapses, these are almost always ironed out in the interception agencies themselves or in the Secretary of State's department before the application reaches the relevant Secretary of State.

3.40 The Secretaries of State themselves are entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information. Since a warrant cannot be issued for a shorter period than the statutory period, Secretaries of State sometimes require a report to be made to them within a short time period - for example after 1 or 2 weeks - of the effectiveness in practice of the warrant. This is with a view to its possible cancellation if in the light of experience it can no longer be properly justified.

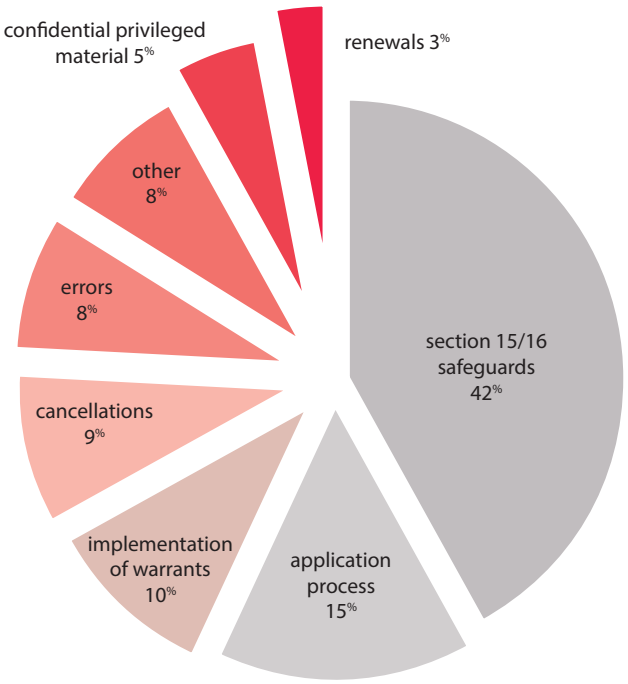
3.41 The total number of specific recommendations made in our inspection reports for the 9 interception agencies was 65, on average about 7 recommendations for each agency. Figure 2 (overleaf) shows the breakdown of recommendations by category.

3.42 Some of the 65 are the same recommendation for more than one agency, for example that the agency should keep its Retention, Storage and Destruction policy and schedule up to date for my continuing inspection (see my investigation on this in paragraphs 3.48 to 3.57 of this report).

3.43 I have expressed concern with a number of areas of the authorisation process, for example, delays in the serving of the warrant instruments (and schedules) on the Communication Service Providers (CSPs).

3.44 I regarded as unsatisfactory the fact that a number of the interception agencies have to apply to renew their warrants excessively early. This results in significantly shortened periods of authorisation. In some cases the applicants have to prepare their renewals a number of weeks before they are due to enable them to be processed in time. Serious crime warrants can only be authorised for a 3 month period. This means that an applicant may have to submit renewal paperwork only a few weeks after the interception was initially authorised. Understandably in some cases there has not been sufficient time

Figure 2 *Interception Recommendations by Category*



to gain a detailed intelligence picture and as a result it can be hard to articulate the benefit and justify the continuance. In addition renewing early causes the intervening authorisation period to be lost and therefore warrants of this kind are frequently not in force for the full 3 month period. A further consequence of early renewal is that warrants are often subject to unnecessary renewals. This places a burden on the interception agencies and the Secretary of State and a strain on the system. There is a strong practical case for increasing the validity period for serious crime warrants to 6 months.

3.45 For some of the interception agencies I was not satisfied that all applications to cancel warrants which were no longer necessary were being made promptly. There was also a delay in effecting cancellations in one of the Secretary of State's departments. The second of these has been addressed. I have recommended that the agencies in question

should be more scrupulous in applying for the cancellation of a warrant which is no longer necessary for a statutory purpose. In almost all such instances the cancellation is a paper formality (albeit a statutory necessity), because the actual interception will have been stopped by technical intervention. But I have regarded these necessary formal cancellations as important. Otherwise there is a rather greater risk of error (as in fact happened in at least one instance during the year).

3.46 I made recommendations to ensure that the required procedures for the handling of confidential privileged material are properly observed. There are detailed requirements on this subject in Chapter 3 of the Interception of Communications Code of Practice, which include the circumstances in which the interception of confidential privileged material have to be brought to my attention.

3.47 My impression is that the interception agencies and the Secretaries of State appreciate the inspection reports. We shall continue to issue them and in the process refine their form and content. A large number of the recommendations have already been addressed by the interception agencies or Secretary of State departments or, if not, I have been assured that work is underway to achieve them. Some require changes to systems and processes which will take time to achieve. I will check progress during my first round of 2014 inspections.

Retention, Storage and Destruction of intercepted material and related communications data

3.48 I decided soon after I was appointed to conduct a detailed investigation into the arrangements for Retention, Storage and Destruction of intercepted material and related communications data by each of the 9 interception agencies. I decided to do this, as it happened, before the media disclosures started, because it seemed to me to be relevant generally to compliance with the statutory safeguards. The formal requests were made afterwards in August 2013 and with an eye to some of the disclosures. This investigation was in addition to my routine inspections of these agencies.

3.49 **My request for information**. I sent a common letter to each of the 9 interception agencies. This asked them to provide full and systematically organised information about the Retention, Storage and Destruction of the product of interception for all relevant interception operations. I asked for particular reference to every database in which intercepted material and related communications data is stored.

3.50 My letter required the interception agencies to have an eye to section 15(3) of RIPA 2000, which provides:

> *"The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy, made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."*

3.51 I explained my reasons for this as including my perception that there was understandable public concern about the necessity and proportionality and the potential intrusion caused by interception of communications on the scale which the agencies were believed to engage in. This included my understanding that the true heart of this concern was (or might be) a general relatively uninformed fear that large scale interception by government controlled agencies might risk providing the government, a future government, the interception agencies, malign individuals or conceivably cyber intruders with an opportunity or ability to intrude ("snoop") into the private lives of individuals who have no connection with any threat to national security, serious crime or any other justifiable statutory purpose for interception.

3.52 My thought was that a full understanding by me of the Retention, Storage and Destruction of intercepted material was central to an appreciation of such potential intrusion as there might be. This should enable me to inform the Prime Minister in appropriate terms (and, through him, the public) of the true informed measure of any justifiable public fear in this respect. I explained that if I were not myself satisfied in any respect, I would require that the agency take steps to achieve compliance.

3.53 **The responses.** All 9 interception agencies responded to my requests in full and with full cooperation. In the result my office now has, and I have fully considered, tabulated information on this topic containing specific answers to all the questions by all the agencies. For obvious reasons of sensitivity, I cannot make public individual details, but I am able to say the following:

- there is a variety of different retention and storage systems used by each of the interception agencies. These have developed over time to accommodate the nature of the different operations which they undertake. There is thus unsurprisingly little consistency in detail;
- none of the interception agencies retain and store for more that a short period the contents of intercepted communications which do not relate to a warranted target or which are of no legitimate intelligence interest. In some systems irrelevant content is deleted manually, in others automatically. A typical period is 24 hours, although some are shorter than this and others rather longer. For example, an interception agency may delete the content of the intercepted communications of a warranted suspected serious criminal straight away if they are not of intelligence interest;
- as to the content of communications which do relate to a warranted target and which are of legitimate intelligence interest, retention periods again vary depending on the legitimate intelligence use to which this may be put. But section 15(3) of RIPA 2000 applies to it and my investigations have satisfied me that its provisions are properly observed. For example, an interception agency may delete the content of the intercepted communications of a warranted suspected serious criminal that are of legitimate intelligence interest when the target is arrested and charged or when the relevant operation comes to an end;
- lawfully intercepted related communications data may in some interception agencies and for technical reasons be stored separately from the content

with longer retention periods. I have recognised that there may be legitimate differences of opinion as to what periods should be applied.

3.54 Having received this tabulated information, I was able to discuss it in detail with each of the interception agencies during my autumn 2013 inspections. I received technical briefings from systems administrators and IT staff and demonstrations where relevant. This enabled me to report back to the interception agencies with a summary of my understanding of their systems in this respect and, in some instances, recommendations for adjustments.

3.55 What this investigation has demonstrated is that indiscriminate retention for long periods of unselected intercepted material (content) does not occur. If it did, it would be a breach of section 15(3) of RIPA 2000. The interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of RIPA 2000.

3.56 Lawfully intercepted related communications data are in some instances retained for a variety of longer periods. On this point, I have yet to satisfy myself fully that some of the retention periods are justified. To an extent, this is work in progress which I shall carry forward. I have made some recommendations in this area and I have required the relevant agencies to report back to me on their progress. In the main, the recommended adjustments comprise a shortening of some individual retention periods or, if not, providing me with more persuasive reasons for keeping the current periods. I shall report further in due course once this work is completed.

3.57 I have in addition asked all the interception agencies to maintain their tabulated schedules and keep them up to date.

Interception Errors

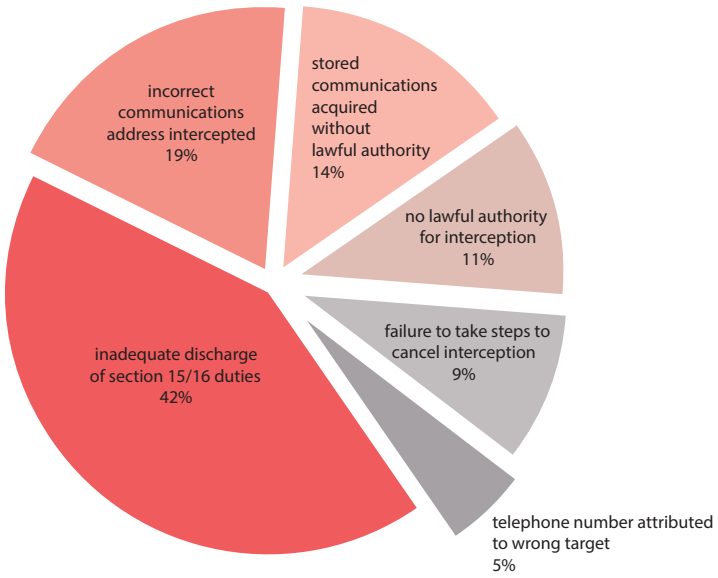
3.58 It is my duty under sections 58(2) and (3) of RIPA 2000 to report to the Prime Minister any contravention of the provisions of the Act, or, any inadequate discharge of section 15 duties (safeguards).

3.59 My predecessors have disclosed the number of errors that have been reported to them each calendar year. This is in principle straightforward for Chapter II communications data, but less so for the interception of communications. This is because, although there is specific provision for errors in the Acquisition and Disclosure of Communications Data Code of Practice (paragraphs 6.9 - 6.25 refer), there is no similar provision in the Interception of Communications Code of Practice. As a consequence there is no mention of the word "error" or related definition for interception. This leaves the interception agencies and my office struggling with an ill-defined framework. However, in my experience the interception agencies are keen to come forward and report to my office any instances which they judge to be errors.

3.60 Even though I am satisfied there is a good culture of self reporting, investigations by my office this year have identified that there is a lack of consistency in relation to the types of instances that are reported. This is because different thresholds and judgments are applied by each interception agency.

3.61 It is my view that there should be an equivalent error provision in the Interception of Communications Code of Practice to that in the Communications Data Code of Practice. Since errors are not easily classified, it requires a lot of thought as to how that provision should be expressed. In the absence of this I will be seeking to agree a memorandum of understanding in this area with the interception agencies to ensure there is consistency in the judgments that are applied and ultimately the errors that are reported. The consultation between my office and the interception agencies on this subject to date has

Figure 3 *Breakdown of Interception Errors*



indicated that this initiative would be welcomed.

3.62 With the preceding paragraphs in mind, the total number of interception errors reported to our office during the calendar year was 57. The breakdown of the causes of these errors is contained in Figure 3.

3.63 66% of the errors were attributable to the interception agencies and 20% to the Communication Service Providers (CSPs) when giving effect to an interception warrant. 14% of the errors were caused by police forces not having the necessary authority in place to access stored communications from mobile devices or computers (i.e. text messages, voice mails and emails). It is important to note that these errors were not made by the interception agencies in relation to lawful interception warrants.

3.64 The largest category of errors is identified as *'inadequate discharge of sections 15/16 duties'*. This is a wide category and can mean different things. One example might be where an analyst had continued to select the communications of an individual based overseas after the individual was known to have entered the UK. Another might be where a technical system malfunctioned causing it to select unwanted data for examination. In these instances the communications had been lawfully intercepted under a section 8(1) or 8(4) warrant, but the resultant action was a breach of the section 15 safeguards. Where necessary I have been satisfied that technical system faults have been fixed or analysts have undertaken further training and supervision to prevent recurrence.

3.65 Although looking at the causes of the errors is of importance in order to take steps to prevent recurrence, it is equally important to consider the consequences of the errors. Where errors are caused by a single technical fault, there may be many consequences. Where communications have been wrongly intercepted, the consequences could be serious.

3.66 On occasions errors occur which are not the responsibility of the interception agencies. For example in one instance the interception agency received the telephone number to be intercepted in good faith from another agency. It subsequently transpired that the other agency had made a transposition error. In this example the Secretary of State gave proper consideration to all of the relevant facts in the interception application and lawfully authorised the warrant – but the telephone number did not in the end relate to the individual of interest. There has been ambiguity in the past as to whether errors of this kind should be reported. They do not constitute contraventions of the Act as the conduct had lawful authority. But I consider that such instances should be reported where they have resulted in unintentional invasion of privacy.

3.67 We have also come across instances where typographical errors have occurred on warrantry paperwork, but where no consequence followed because they were identified and rectified and never acted on. I do not consider that these need to be reported. But the interception agencies should still take steps to ensure so far as is possible that mistakes of this kind do not occur, since they could have serious consequences.

3.68 In the majority of instances I was satisfied with the timeliness of the error reports received by my office. However, I raised concerns with two of the interception agencies on this point. Some of the more complicated technical errors may understandably take time to investigate fully. In these cases I agreed that the agencies could send me an initial notification at the point at which it is clear that an error has occurred and then follow this up with a full report once the cause of the error has been fully ascertained and the measures put in place to prevent recurrence. In the more straightforward cases I would expect to receive a full report straight away and systems have been put in place at the agencies to ensure that this now happens.

Points of Note

Interception of Communications

2760 interception warrants (to access the content of communications) were authorised in 2013, a reduction of 19% on the previous year.

In 2013 I conducted 26 interception inspections. During the inspections 600 interception warrants were examined which is one third of the extant warrants at the end of the year.

A total of 65 recommendations emanated from these inspections, on average 7 recommendations for each interception agency.

In 2013 and since, I have conducted a number of further detailed interception investigations. A number of these related to media publications based on disclosures reportedly made as a result of Edward Snowden's actions. These feature in Section 6 of this report as Questions of Concern.

My investigation into the Retention, Storage and Deletion of intercepted material and related communications data has demonstrated that:

- indiscriminate retention for long periods of unselected intercepted material (content) does not occur. The interception agencies delete intercepted material (if it is retained at all) after short periods and in accordance with section 15(3) of RIPA;
- related communications data are in some instances retained for a variety of longer periods. I have yet to satisfy myself fully that some of these periods are justified and in those cases I have required the agencies to shorten their retention periods or, if not, provide me with more persuasive reasons for keeping the material for the current periods.

57 interception errors were reported to our office in 2013. There is no specific provision in the Interception of Communications Code of Practice for errors and this leads to a lack of consistency in the reporting. In the absence of a specific provision I will be seeking to agree a memorandum of understanding with the agencies.

Our inspections and investigations lead me to conclude that the Secretaries of State and the agencies that undertake interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest. This is subject to the specific errors reported and the inspection recommendations. These require attention but do not materially detract from the judgment expressed in the first sentence.

Section 4
Communications Data

4.1 In this section I shall provide an outline of the communications data legislation, give details in relation to our communications data inspection regime and summarise the key findings from our inspections.

4.2 RIPA 2000 Part I Chapter II (sections 21 to 25) concerns the acquisition and disclosure of communications data. Communications data colloquially embrace the 'who', 'when' and 'where' of a communication but not the content, what was said or written. Put shortly, communications data comprise of the following.

- *Traffic data* which is data that may be attached to a communication for the purpose of transmitting it and could appear to identify the sender and recipient of the communication, the location from which and the time at which it was sent, and other related material (see sections 21(4)(a) and 21(6) and (7) RIPA and Paragraphs 2.19 to 2.22 of the Communications Data Code of Practice).
- *Service use information* which is data relating to the use made by any person of a communication service and may be the kind of information that habitually used to appear on a Communications Service Provider's (CSP's) itemised billing document to customers (see section 21(4)(b) and Paragraphs 2.23 and 2.24 of the Communications Data Code of Practice).
- *Subscriber information* which is data held or obtained by a CSP in relation to a customer and may be the kind of information which a customer typically provides when they sign up to use a service. For example, the recorded name and address of the subscriber of a telephone number or the account holder of an email address. (See section 21(4)(c) and Paragraphs 2.25 and 2.26 of the Communications Data Code of Practice).

Applications for Communications Data

4.3 There are a number of public authorities with statutory power to apply for communications data under Chapter II. These include:

- Police forces
- National Crime Agency (NCA)
- Her Majesty's Revenue and Customs (HMRC)
- Security Service (Mi5)
- Secret Intelligence Service (Mi6)
- Government Communications Headquarters (GCHQ),

4.4 In addition, there are other public authorities specified under section 25(1) by order of the Secretary of State. The additional public authorities are listed in the Regulation of Investigatory Powers (Communications Data) Order 2010 (Statutory Instrument No. 480).

4.5 Annex A provides tabulated details of the additional public authorities with statutory power to acquire communications data given to them by Parliament to enable them to carry out their public responsibilities. As I will outline later in this section, around one third of these public authorities actually acquired communications data in 2013.

4.6 The giving of lawful authority for acquiring communications data is set out in the statute and is undertaken by a senior designated person (DP) within the public authority acquiring it. Under Part I Chapter II and the associated Code of Practice there has to be;

- **an applicant**, a person who wants to acquire the communications data for the purpose of an investigation. The applicant has to complete an application form. The application must provide in structured form the details required by paragraph 3.5 of the Code of Practice.
- **a designated person (DP)**, who is a person holding a prescribed office in the relevant public authority. The DP's function is to decide whether authority to acquire the communications data should be given. Their function and duties are described in paragraphs 3.7 to 3.14 of the Code. Except where it is unavoidable or for reasons of urgency or security, the DP should not be directly involved in the relevant investigation. The DP has to decide whether it is lawfully necessary and proportionate to acquire the communications data to which the application relates.
- **a single point of contact (SPoC)** who is an accredited individual or group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Their functions are described in paragraph 3.15 to 3.21 of the Code – see in particular the list of functions in paragraph 3.17. These include:
  - advising both applicants and DPs on the interpretation of RIPA 2000 Part I Chapter II, in particular whether it is appropriate to give the authority; and
  - providing assurance to DPs that the application is free from errors and that granting it would be lawful under the Act.
- **a senior responsible officer (SRO)** within the public authority, who is responsible for the integrity of the process within that public authority to acquire communications data and for compliance with Part I Chapter II of the Act and the Code of Practice.

4.7 Essentially there are two methods for acquiring communications data – an authorisation under section 22(3) or a notice under section 22(4). An authorisation is effected by a person from the relevant public authority engaging in conduct to acquire the communications data. A notice is effected by requiring a CSP to disclose the data to the relevant public authority.

4.8 An authorisation or notice to acquire communications data must comply with the formalities required by section 23(1) to (3) of RIPA 2000. They have a maximum period of validity of one month (section 23(4)) and may be renewed by the same procedures under which they were given in the first place (section 23(5)). There are provisions for cancellation if it is no longer necessary or proportionate to acquire the communications data.

4.9 **Necessity.** The mechanism by which a DP may give authority to obtain communications data requires that person to believe that it is *necessary* to obtain it for one or more of the statutory purposes set out in section 22(2) of RIPA 2000. These are:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic wellbeing of the United Kingdom;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
- for any purpose (not falling within the above which is specified for the purpose of this subsection by an order made by the Secretary of State – see paragraph 2.2 of the Code of Practice for these).

4.10 Parliament prescribed restrictions on the statutory purposes for which public authorities may acquire communications data and also on the type of data that can be acquired. For example, local authorities can only acquire service use and subscriber information for the purpose of *"preventing or detecting crime or of preventing disorder."*

4.11 Annex A provides details of the types of data and the statutory purposes under which each public authority can acquire that data in tabulated form.

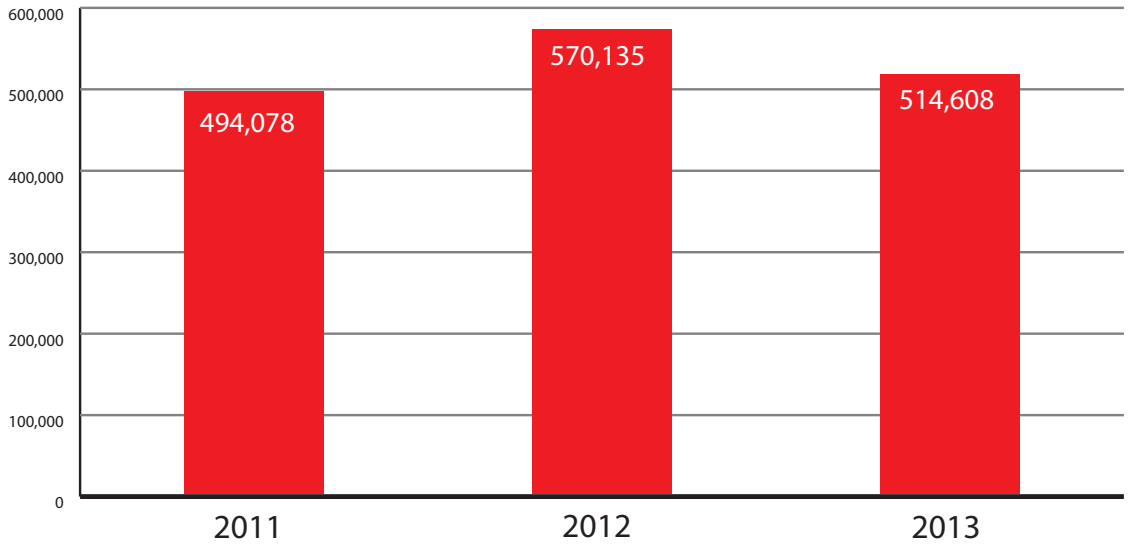
4.12 **Proportionality.** A DP is forbidden from approving an application for communications data unless he believes that obtaining the data in question, by the conduct authorised or required, is proportionate to what is sought to be achieved by so obtaining the data. Thus every application to acquire communications data has to address proportionality explicitly.

4.13 A judgment whether it is proportionate to authorise the acquisition of communications data requires holding a balance between (a) the necessity to engage in potentially intrusive conduct and (b) the anticipated amount and degree of intrusion. The judgment has to consider whether the information which is sought could reasonably be obtained by other less intrusive means. Applications for communications data are refused (or not applied for) where it is judged that the necessity does not outweigh the intrusion. An application is more likely to be granted for a mobile telephone which a suspect is known to use for criminal purposes than if the telephone may also be used by other members of the target's family as well. That said, it is unavoidable that unconnected and intrusive data may be acquired. Judging the likely intrusion in advance is not an exact science.

Statistics for Communications Data

4.14 Figure 4 shows the number of authorisations and notices for communications data over the previous three years (excluding urgent oral applications). The total number approved in 2013 was 514,608.

Figure 4 *Total Notices & Authorisations under RIPA 2000 Part I Chapter II 2011-13 (excluding urgent oral)*



4.15 The urgent oral process is used to acquire communications data where there is no time to complete the normal written process. For example, in circumstances where there is an immediate threat to life, an urgent operational requirement relating to serious crime or a credible threat to national security. In 2013 there were 42,293 notices and authorisations given orally.

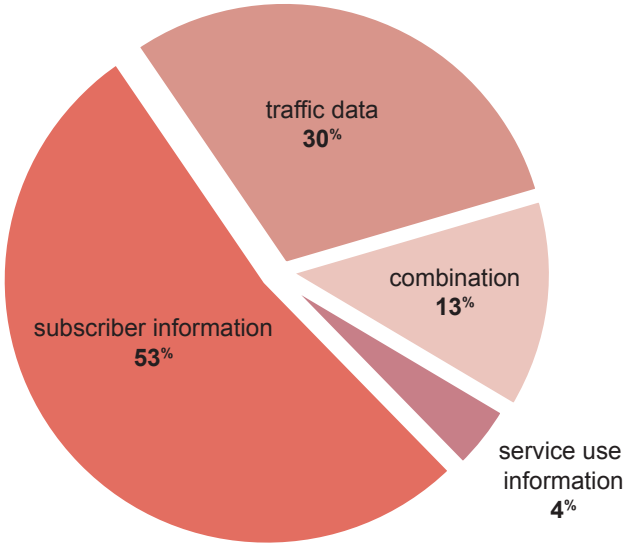
4.16 It is not presently possible to report the number of individuals to which the 514,608 notices and authorisations relate, but that number would be much smaller. Public authorities often make multiple requests for communications data in the course of a single investigation, but also make multiple requests for communications data in relation to the same individual.

4.17 Figure 5 shows the breakdown of notices and authorisations by type of data under section 21(4). Over half of the requirements were for subscriber information under section 21(4)(c). The breakdown is much the same as for 2012.

4.18 My predecessor referred to the inadequacy of the statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice in his 2012 annual report. The requirement is contained in Paragraph 6.5 of the Code of Practice, but

essentially the public authorities are only required to report the number of authorisations and notices (written and oral) and the number of applications rejected.

Figure 5 *RIPA 2000 Part I Chapter II Authorisations & Notices by Data Type*



4.19 The statistical information required by the Code of Practice is flawed for the following reasons:

- more than 1 item of data may be requested on an authorisation or notice and therefore the number of individual items of communications data requested is not reported. It is likely that this figure would be higher than the number of authorisations and notices.
- the different workflow systems in use by public authorities have different counting mechanisms for notices and authorisations. For example, one public authority may request data in relation to 3 telephone numbers on 1 notice, whereas another public authority may request the same 3 items of data on 3 separate notices. The result would be an over inflated number of authorisations and notices for the second public authority. This makes meaningful comparisons difficult.
- it is a requirement for public authorities to report the number of applications that have been *rejected* each calendar year, but not the number of applications that were approved. Therefore it is difficult to establish accurately the percentage of applications rejected.

4.20 We have consulted with the Home Office and set out the revisions and enhancements of the statistical requirements that we believe are necessary both to assist us with our oversight role, and, to inform the public better about the use which public authorities make of communications data. The suggested enhancements include

requirements for:

- the total number of applications submitted,
- the total number of items of data requested,
- the total items of data broken down by statutory necessity purpose (i.e. prevent / detect crime, national security etc.)
- the total items of data broken down by crime type or other purpose (i.e. murder, robbery etc).

4.21 In my view the unreliability and inadequacy of the statistical requirements is a significant problem which requires attention.

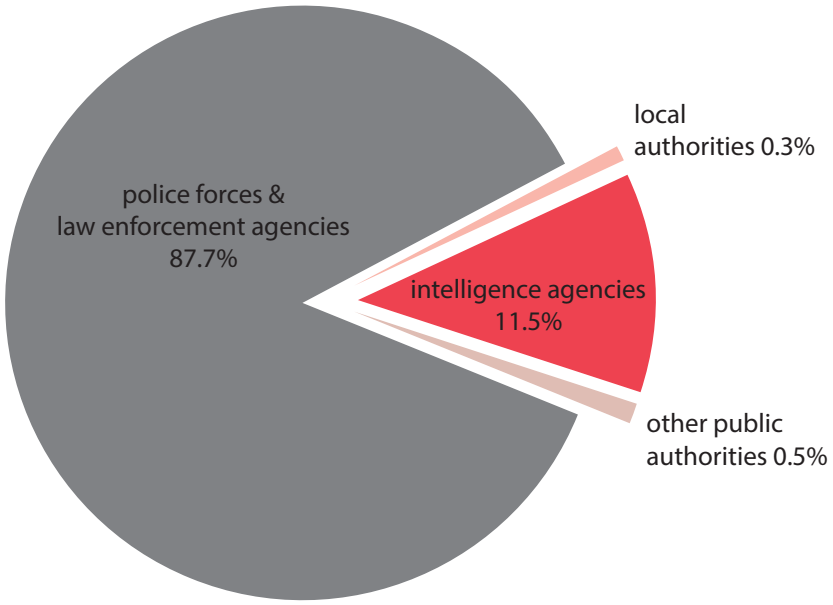
4.22 We are aware that a number of CSPs are releasing transparency figures in relation to the communications data disclosures they make to public authorities. These statistics should be treated with caution as again different counting mechanisms and rules are applied which can lead to misleading comparisons. In my view the statistical information should be collected by the public authorities, under required conventions and counting mechanisms to ensure that it is comparable and accurate.

4.23 Taking these difficulties into account, it is with considerable caution that I have decided to publish further statistical information in this report. The public authorities are not mandated to provide some of this statistical information and as a result it has not been easy, or in some cases possible, to extract the information from their systems. The public authorities all, without question, considered my request for further statistical information as part of their general duty under section 58(1) of RIPA to disclose or provide to me all information I may require to carry out my function. With that in mind they have been extremely helpful in making available what further statistical information they could. In particular some police forces experienced significant difficulties and were unable to provide enhanced statistics without examining each individual application. It is not feasible to count thousands of requests manually and therefore some of the further statistical information I publish in this report is based on samples of the overall total.

4.24 Figure 6 shows the breakdown of the 514,608 notices and authorisations by type of public authority. It will be seen that 87.7% of these were made by police forces and law enforcement agencies. Less than 1% were made by local authorities and 'other' public authorities. 'Other' public authorities include regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions. This breakdown must be treated with caution for the reasons outlined in the preceding paragraphs.

4.25 Annex B of this report provides a breakdown of the 514,608 notices and authorisations by public authority. It is only indicative of the amount of communications data acquired by these public authorities and must be treated with caution for the reasons outlined in the preceding paragraphs. It is important therefore that the numbers are not used inappropriately to produce league table comparisons.

Figure 6 *2013 Proportion of Authorisations & Notices under RIPA 2000 Part I Chapter II by Public Authority Type*



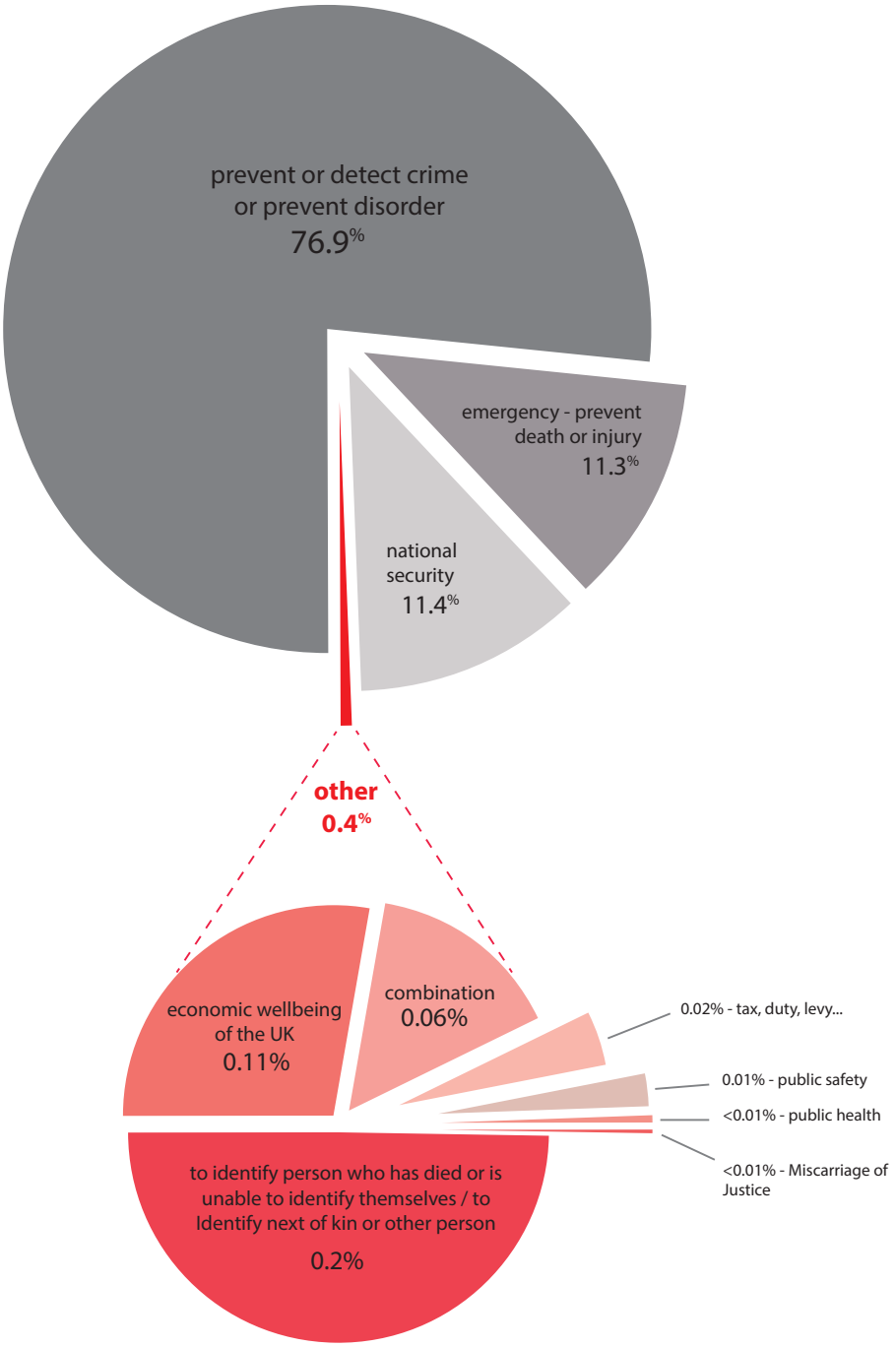
4.26 Finally, this year my office conducted a scoping exercise for this report with the aim of providing some further statistical information in relation to the statutory necessity purposes under which data is required. There has in the past been legitimate public concern expressed in relation to the allegedly large number of statutory necessity purposes for acquiring communications data. What my scoping exercise has shown is that less than half a percent of all the requests were for purposes other than the prevention and detection of crime or the prevention of disorder, national security, or in an emergency to prevent death or injury. Figure 7 (overleaf) details this breakdown which, although representative, must again be treated with caution for the reasons outlined in the preceding paragraphs.

Question of Concern

4.27 There is a question of concern I have raised in public as a possibility. It will require detailed examination which we are in the process of undertaking.

4.28 The communications data statistics given above are liable to be misleading. But taking the 514,608 number for Part I Chapter II authorisations and notices at face value, it seems to me to be a very large number. It has the feel of being too many. I have accordingly asked our inspectors to take a critical look at the constituents of this bulk to see if there might be a significant institutional overuse of the Part I Chapter II powers. This may apply in particular to police forces and law enforcement agencies who between them account for approaching 90% of the bulk.

Figure 7 *2013 Total Notices & Authorisations under RIPA 2000 Part I Chapter II by Statutory Purpose*



Caveat: This chart is created to give indicative proportions of which statutory purpose the Notices given and Authorisations granted in 2013 were for. The statistical difficulties are explained in the text. The main point is that the contribution from a significant number of Police Forces has to be by extrapolations from a smaller sample of forces that are able to give an accurate breakdown.

4.29 I do not consider that this is a matter that can properly be scrutinised by looking only at individual requests, which, taken alone, may be entirely justified. It is, I think, necessary to take a much broader view of institutional assumptions and use. Since a very large proportion of these communications data applications come from police and law enforcement investigations, it may be that criminal investigations generally are now conducted with such automatic resort to communications data that applications are made and justified as necessary and proportionate, when more emphasis is placed on advancing the investigations with the requirements of privacy unduly subordinated.

4.30 The SPoCs have an essential role to play here in using their experience to challenge the investigative strategy underlying the applications which they oversee. Of course it is not their task to impede the proper progress of criminal investigations. This particularly applies to applications which are properly urgent, for instance, if there is a kidnapping or a life at risk. But our inspectors have found instances where applications are marked urgent when in truth they are not, or where there has been delay in making the application. The very fact of delay sometimes suggests that the necessity for the application may be questionable. More generally, a proper regard for privacy could mean that a proportion of applications currently routinely promoted as necessary could be seen as inadequately justified.

4.31 I will report on this inquiry when my investigation is complete, but in any event in my report for 2014.

Inspection Regime

4.32 **Objectives of the inspections.** 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;
- that all acquisition of communications data has been carried out lawfully and in accordance with Part I Chapter II and its associated Code of Practice;
- that the data acquired was necessary and proportionate to the conduct authorised;
- that errors are being 'reported' or 'recorded' and that the systems are reviewed and adapted in the light of any exposed weaknesses or faults.
- that persons engaged in the acquisition of data are adequately trained and are aware of the relevant parts of the legislation.

4.33 **Number of inspections.** The 8 full time inspectors undertake the communications data inspections. In 2013 our office conducted 75 communications data inspections broken down as follows: 43 police force and law enforcement agency, 1 intelligence agency, 17 local authority and 14 'other' public authority inspections. Communications

data inspections of the other two intelligence agencies happened to fall just outside the calendar year 2013.

4.34 An additional 130 local authorities were inspected during the National Anti Fraud Network (NAFN) inspection. NAFN continues to provide a SPoC service for local authorities and 85% of the local authorities that reported using their powers in 2013 submit their requirements via the NAFN SPoC. Our inspection of NAFN itself showed very good compliance and we continue to encourage all local authorities to use their services. There are strong practical reasons for NAFN's legislative remit to be enlarged to embrace other public authorities who are infrequent users of RIPA 2000 Part I Chapter II. This view was shared by the Joint Parliamentary Committee which scrutinised the then draft Communications Data Bill.

4.35 The length of each inspection depends on the type of public authority being inspected and their communications data usage. The inspections of the larger users, such as police forces, are conducted by at least two inspectors and take place over 3 or 4 days. The inspections of the smaller volume users are conducted by one inspector and generally last 1 day.

4.36 Examination of systems and procedures for acquiring communications data. Our communications data inspections are structured to ensure that key areas derived from Part I Chapter II and the Code of Practice are scrutinised. The larger users have bespoke workflow systems to manage their applications for communications data and the inspectors have full access to those systems and interrogate them. A typical inspection may include the following:

- a review of the action points or recommendations from the previous inspection to check they have been implemented.
- an audit of the information supplied by the CSPs detailing the requests that public authorities have made for disclosure of data. This information is compared against the applications held by the SPoC to verify that the necessary approvals were given to acquire the data.
- examination of individual applications for communications data to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements.
- scrutinising at least one investigation or operation from start to end to assess whether the communications data strategy and the justifications for acquiring all of the data were proportionate.
- examination of the urgent oral approvals to check the process was justified and used appropriately.
- a review of the errors reported or recorded, including checking that the measures put in place to prevent recurrence are sufficient.

4.37 **Samples**. I have previously said (in relation to interception warrants) that it is important that we scrutinise a sufficient sample of the individual applications. But, in my view, inspecting and understanding systems is in the end more important than scrutinising yet more individual applications. That said, it is generally feasible in the smaller public authorities for our inspectors to examine all of the applications submitted in the period being examined.

4.38 For the larger users, sampling must be undertaken. A survey conducted by our office estimated that approximately 10% of the applications *submitted* in the period being examined are individually scrutinised during the inspections of the larger users. If the number of applications submitted by public authorities was one of the statistical requirements of the Code of Practice, this estimate would be more accurate. In any event, the inspectors randomly sample thousands of individual applications each year. It is also worth noting the following points in relation to the *random* sampling:

- it is conducted at both ends of the process – i.e. from the public authority records and the data obtained from the CSPs;
- if the inspectors identify an error or issue during the random sampling which may impact on other applications, the public authority is required to identify other applications which may contain the same error or fault. Therefore, although random sampling may only pick up 1 error, this will lead to all error instances of that type being investigated and reported;
- the inspectors will continue to examine applications until they reach the point that they are satisfied that what they have examined is an accurate representation of the public authority's compliance.

4.39 In addition to the random sampling, where possible the Inspectors also conduct *query based searches* across the workflow systems. The query based searches enable specific areas to be tested for compliance. For example, a DP query based search relating to a particular DP enables the inspectors to scrutinise the quality of the DPs considerations in relation to necessity and proportionality, check that the DPs are not rubber stamping applications and that the DPs are of the appropriate rank or level to act in that capacity. Another example might be a query based search to identify any requests where data has been applied for over lengthy time periods or where particularly intrusive data sets have been acquired. This type of sampling not only enables key themes to be examined, but also enables identified parts of a larger number of applications to be examined. Our office has been consulting with the workflow providers to enable the examination of a wider cross section of applications and they have been very willing to assist in this respect.

4.40 **Inspection Reports**. The reports contain a review of compliance against a strict set of baselines that derive from Part I Chapter II and the Code of Practice. They contain formal recommendations with a requirement for the public authority to report back within two months to say that the recommendations have been implemented, or what progress has been made.

4.41 Inspection Findings and Recommendations. The total number of recommendations made during our 75 communications data inspections in 2013 was 299 (Figure 8). A traffic light system (red, amber, green) is in place for the recommendations to enable public authorities to prioritise the areas where remedial action is necessary:

- Red recommendations - immediate concern - serious breaches and / or non-compliance with Part I Chapter II or the Code of Practice.
- Amber recommendations - non-compliance to a lesser extent; however remedial action must still be taken in these areas as they could potentially lead to serious breaches.
- Green recommendations - represent good practice or areas where the efficiency and effectiveness of the process could be improved.

This year 19 (6%) of the recommendations were red, 177 (59%) amber and 103 (35%) green. Comparisons with previous years are difficult because the public authorities being inspected are not the same and the number of inspections conducted each year differs. However, in 2013 the inspectors made on average fewer recommendations per inspection than in 2011 & 2012. The proportions of red, amber, green have remained broadly the same.

Figure 8 *Total red, amber & green recommendations resulting from communications data inspections 2011-2013*

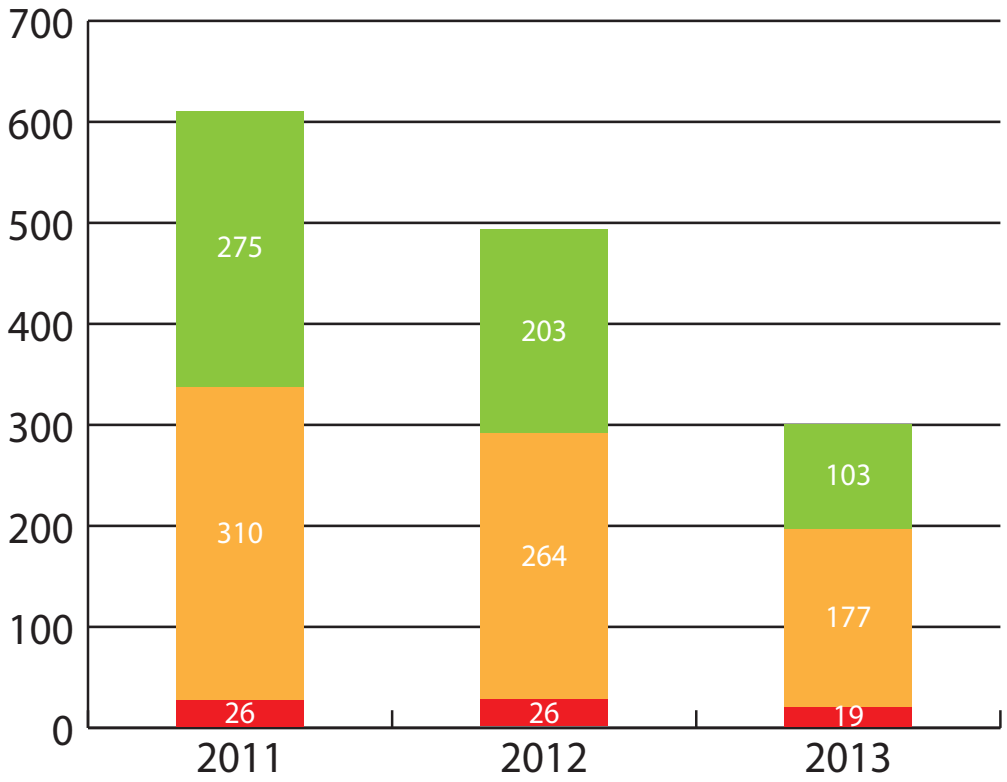
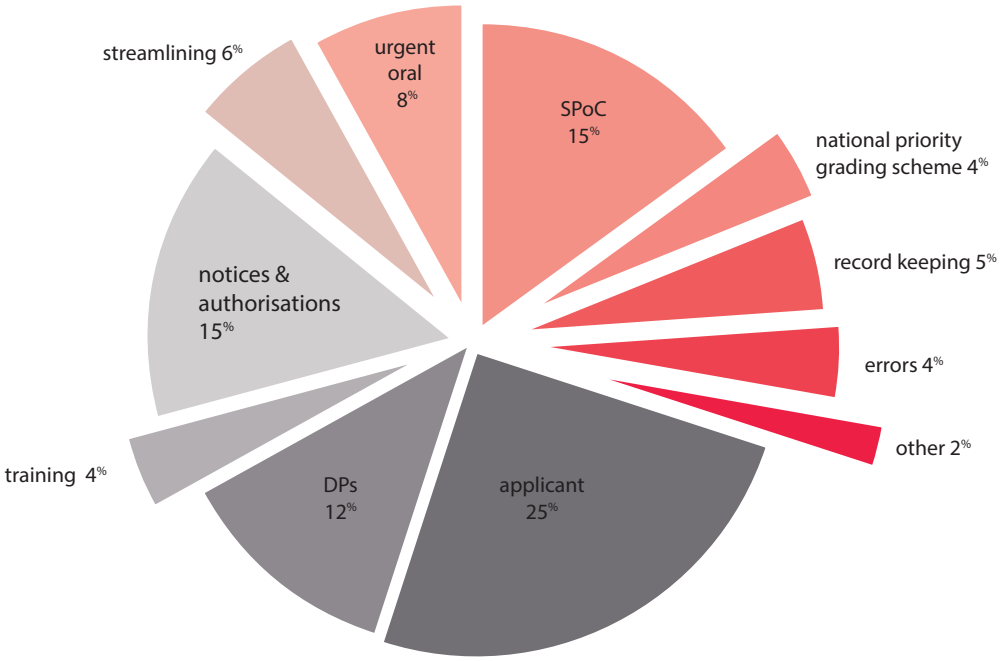


Figure 9 *Communications Data - 2013 Inspection Recommendations by Category*



4.42 Figure 9 shows the breakdown of the 2013 recommendations by category. Almost 70% of the recommendations fell into 4 key categories:

(1) **Applicant.** The majority of the recommendations in this category focused on the necessity or proportionality justifications set out by the applicants. The inspectors made recommendations in approximately a third of the public authorities inspected around these two key principles as they could not be satisfied in every instance that the applicants had sufficiently justified them.

One example might be that it was not clear how the request for data met the section 22(2) necessity test as the criminal offences under investigation had not been clearly set out in the application. Another example might be where the data requested did not appear to be a proportionate response to the matter under investigation as the applicant had failed to explain how the time period was relevant or what they were aiming to achieve from obtaining that data set and how that would benefit the investigation.

These issues did not affect all applications submitted by the public authority. However they were prevalent enough across the samples examined for the inspectors to consider that a recommendation was necessary. In such instances the inspectors will seek further supporting documentation (such as case file, policy logs etc.) or interview the applicant or DP to satisfy themselves that the requests were necessary and a proportionate response.

(2) **Single Point of Contact (SPoC)**. The majority of the recommendations in this category fell into two key areas; guardian and gatekeeper role and efficiency.

The SPoC has an important guardian and gatekeeper role to perform to ensure that the public authorities act in an informed and lawful manner when acquiring communications data. The overall picture is that the SPoC process is a stringent safeguard. However, recommendations were made for the SPoC to exercise their guardian and gatekeeper role more robustly in a small number of the inspections.

In the vast majority of inspections the inspectors did see ample evidence of SPoCs challenging applicants in cases where they believed the requirements had not been met. This year our office obtained some further statistical information in relation to the number of applications that the SPoCs are returning for further development or improvement. The figure is not complete, as only the larger users were surveyed and not all could provide the information for reasons I have alluded to earlier in my report. It does indicate however that on average a quarter of applications are returned by the SPoC.

This figure should also be treated with caution as we do not have the reasons for the returns, and some may have been returned for purely administrative reasons or because the data was not available, rather than for quality issues. However, the return rate does provide evidence that the SPoCs are scrutinising and challenging applications. Our inspectors also see evidence of the SPoCs suggesting less intrusive or more effective ways that the applicant might meet their objective.

Our inspections identified that some public authorities were experiencing serious backlogs in dealing with applications due to a lack of staff or inadequate systems in the SPoC. This is concerning as it could have an impact on compliance. In addition it is also questionable whether the necessary and proportionality justifications are still valid in cases where it has taken weeks to process an application.

(3) **Designated Persons (DPs).** The majority of the recommendations in this category fell into three key areas; DP considerations, timeliness of approvals and DP independence.

Overall the inspectors were satisfied that the large majority of DPs had discharged their statutory duties responsibly. There is evidence that the DPs are questioning the necessity and proportionality of the proposed conduct. This year it is possible for me to report the percentage of applications that were rejected or returned for redevelopment by the DPs in the larger public authorities as these were included in my request for further statistical information. In the larger users, 5% of applications were rejected or returned for redevelopment by the DPs.

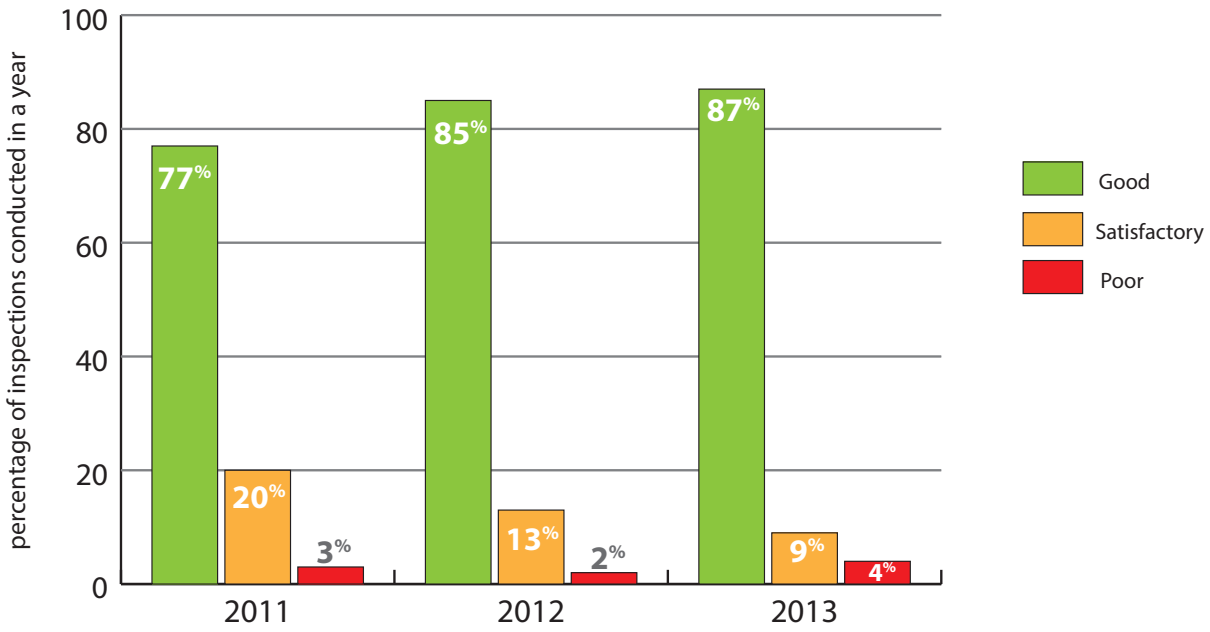
The Inspectors concluded that vast majority of DPs were completing their written considerations to a good or satisfactory standard. Where satisfactory our inspectors highlighted to DPs, as a matter of good practice, how they could further improve their considerations. In a number of public authorities the DPs were not considering the applications in proper time. For a number of reasons it is important for applications to be considered promptly, not least because the necessity and proportionality justifications might become invalid in the intervening period.

Overall there is good level of objectivity and independence in the approvals process, or, where there was not, the individuals were acting for reasons of urgency or security. In a minority of public authorities compliance issues were identified in this area and recommendations resulted.

(4) **Notices and Authorisations.** The majority of the recommendations in this category resulted from misunderstandings in the procedures surrounding granting authorisations and giving notices. I have previously outlined that notices and authorisations are the two methods of conduct to acquire communications data. In certain instances our inspectors identified that the course of conduct approved by the DP was not in the end the course of conduct followed by the SPoC to acquire the data, or, that the correct legal instrument was not served on the CSP to request disclosure of the data. These are technical breaches of Part I Chapter II and the Code of Practice and constitute recordable errors. The reason they are not reportable errors is because the DPs had in fact approved the acquisition of the data as necessary and proportionate and the public authority did not receive any data the acquisition of which had not been approved.

4.43 At the end of each inspection, the individual public authority is given an overall rating (good, satisfactory, poor). This rating is reached by considering the total number of recommendations made, the severity of those recommendations, and whether those recommendations had to be carried forward because they were not achieved from the previous inspection. On the latter point, 95% of the public authorities inspected in 2013 had fully achieved all or the majority of the recommendations emanating from their previous inspection.

Figure 10 *Communications Data - Inspection Ratings 2011-2013*



4.44 Figure 10 shows that overall the number of public authorities achieving a good level of compliance has steadily risen in the last three years.

Communications Data Errors

4.45 There is provision in the Acquisition and Disclosure of Communications Data Code of Practice (Paragraphs 6.9 – 6.25 refer) for errors. There are two categories of errors; reportable and recordable errors.

4.46 **Recordable error.** In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences. These records must be available for our inspections. They must include details of the error and;

- explain how the error occurred,
- provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur.

The public authority's SRO must undertake a regular review of the recording of such errors.

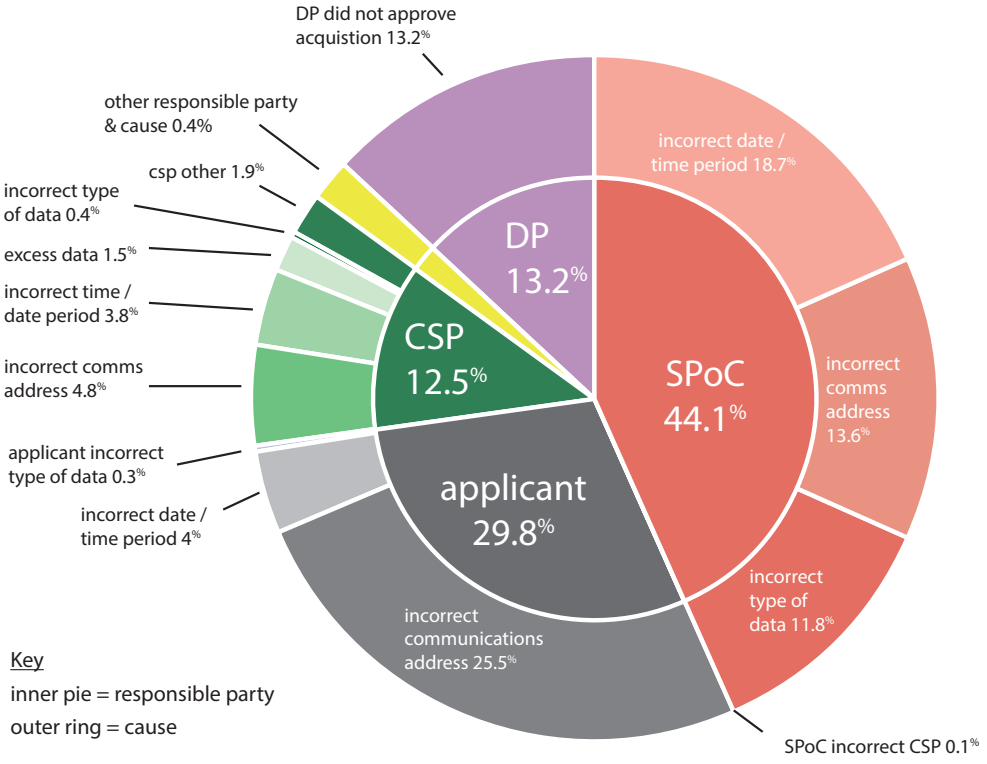
4.47 **Reportable error**. Where communications data is acquired or disclosed wrongly a report must be made to me within no more than five working days of the error being

discovered. (Paragraphs 6.13 & 6.17 of the Code of Practice). The error report must include details of the error and;

- explain how the error occurred,
- indicate whether any unintended collateral intrusion has taken place,
- provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur.

4.48 The total number of communications data errors reported to my office in 2013 was 869. In addition a further 101 were identified during the inspections by our inspectors making 970 reportable errors in all. Some of the 101 errors had already been identified by the public authorities, but had been wrongly classified as recordable errors and our inspectors picked these up when reviewing the public authorities recordable errors register. For example, in some instances the public authorities had noticed and corrected a mistake with the telephone number prior to serving the requirement on the CSP, but had failed to go back to the DP to seek approval for the new number. Technically this data was not acquired fully in accordance with the law as the DP had not given authority for the final communications address. However it was clear in these cases that the DP had approved the necessity and proportionality case. Others had not been identified or realised by the public authorities themselves and this was why they had not been reported before the inspectors identified them. 61 of the 101 errors stemmed from just three applications that were examined during the inspections.

Figure 11 *Breakdown of Errors by Cause and Responsible Party*



4.49 87.5% of the 970 errors were attributable to public authorities and 12.5% to CSPs. Figure 11 (on the previous page) shows the breakdown of errors by responsible party and cause.

4.50 Nearly half of the errors were caused by data being requested on the incorrect communications address. Public authorities and CSPs must take action to reduce these errors. Although I of course appreciate that everyone is human and mistakes will happen from time to time, I do not accept that more cannot be done to reduce such errors occurring. For example, our investigations have shown that in a large number of instances where the applicant put the incorrect telephone number on their application form, the telephone number was available to the applicant in electronic form and could have been copied and pasted into the application. Had this simple step been taken, the error would not have occurred.

4.51 A total of 970 reportable errors has to be taken in the context of all the data derived from a total 514,608 notices and authorisations. Any reportable error is regrettable. The majority of the 970 reportable errors had no serious consequence. I have to report that 7 errors with very serious consequences have occurred this year. Regrettably these errors resulted in police action relating to wrongly identified individuals. In 5 of these cases the mistakes caused a delay in the police checking on young persons who were intimating suicide or on an address where it was believed that someone had been the victim of a serious crime. Fortunately the police were able to identify quickly in these instances that the persons visited were not connected with their investigation. In the remaining instances warrants were executed at the homes of innocent account holders and this is extremely regrettable.

4.52 All but one of these errors occurred in relation to requests for Internet Protocol (IP) data to identify the account that was accessing the internet at a particular date and time. There were 3 specific causes for the errors: data applied for over the wrong date or time, the incorrect time zone conversion or a transposition error in the IP address.

4.53 One of my inspectors has conducted a full investigation into these errors. He has held meetings with the relevant public authorities and CSPs to determine the exact cause and ensure that steps are put in place and systems are changed to prevent recurrence. It is clear that some of the errors could have been avoided if the details had been transferred electronically between systems. Furthermore in some cases the error was actually apparent on the result that was disclosed. It was unsatisfactory in these instances that both the SPoC and the applicant failed to review the result properly and identify the error. Had they done so the resultant police action and serious intrusion into the privacy of innocent individuals would have been prevented. One of the roles of the SPoC as prescribed by the Code of Practice is to assess whether the communications data disclosed or obtained fulfils the requirement of the notice or authorisation. SPoCs must ensure that robust measures are put in place to check results for errors before dissemination. It is fortunate that errors with such severe consequences are very rare, but I believe, as was the case in a number of these instances, that more should be done by the public authorities to ensure they have sufficiently robust systems in place to prevent occurrence.

4.54 My predecessor made 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 for quality to ensure they are functioning effectively. I agree with this and would add that one technical systems error can have wider consequences than one human error. My office is in the process of investigating one such CSP system error which resulted in incorrect data being disclosed to a large number of public authorities. The error in the main caused false negative results to be provided in relation to requests for subscriber information. Accordingly no positive harm resulted to individuals. At the time of writing this report our investigation into the cause and impact of this error is still ongoing.

Points of Note

Communications Data

In 2013, 514,608 authorisations and notices for communications data under RIPA 2000 Part I Chapter II were approved.

214 public authorities acquired data in 2013.

87.7% of the 514,608 authorisations and notices were made by police forces and law enforcement agencies, 11.5% by the intelligence agencies and less than 1% by local authorities and other public authorities (regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions).

The statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice are flawed and inadequate. Our office has consulted with the Home Office and set out the revisions and enhancements that we believe are necessary both to assist us with our oversight role, and, to inform the public better about the use which public authorities make of communications data. The unreliability and inadequacy of the statistical requirements is a significant problem which requires attention.

In 2013 our office conducted 75 communications data inspections. Our inspections are structured to ensure that key areas derived from Part I Chapter II and the Code of Practice are scrutinised. Our inspectors have full access to the workflow systems used by public authorities and interrogate them. 299 recommendations emanated from these inspections, on average 4 recommendations for each public authority.

970 RIPA 2000 Part I Chapter II communications data errors were reported to our office in 2013, 87.5% were attributable to public authorities and 12.5% to Communication Service Providers (CSPs).

Almost half of the errors were caused by data being requested on the incorrect communications address. Public authorities and CSPs must take action to reduce this type of error. Our investigations have shown that in a large number of instances this type of error could have been avoided.

My office is in the process of undertaking an inquiry into whether there might be an institutional overuse of authorisations to acquire communications data under RIPA Part I Chapter 2. I will report on this inquiry when my investigation is complete, but in any event in my report for 2014.

Section 5
Media Disclosures and Public Concerns

5.1 During the second half of 2013 (and since then) there were a series of disclosures in the media said to be derived from Edward Snowden, who was a contractor working at the United States (US) National Security Agency (NSA). Much of what has been reported concerned the alleged operational practices and activities of the NSA or other agencies in the US. Other disclosures concerned alleged UK operational activities, in particular by or relating to GCHQ. Relevant public and parliamentary debate followed and raised a number of legitimate questions.

5.2 Some of the media disclosures and questions concern the interception of communications and, to that extent, I have regarded these matters as within the scope of my statutory oversight responsibility. Obviously, if interception agencies or others are acting unlawfully under RIPA 2000 Part I, I have a duty to report it to the Prime Minister. Other questions may have overtones of policy, which is not perhaps within the literal terms of my statutory function, but there are instances where the borderlines are blurred.

5.3 I have undertaken extensive investigations into the subject matter of the media disclosures with two objectives in mind:

- to investigate and be able to report on the lawfulness (or otherwise) of relevant interception activities which UK interception agencies may undertake or have undertaken.
- to address and report on a variety of concerns which have been expressed publicly in Parliament or in the media arising out of the media disclosures. I have distilled my understanding of a number of those concerns and will address them in this report.

Before doing that there are a few introductory matters.

5.4 **Report to President Obama.** I have read in full the Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies "Liberty and Security in a Changing World" of 12 December 2013. The Group was established and their review commissioned on 27 August 2013 in the wake of Snowden disclosures. It addresses issues some of which are generically much the same as some of those which I have addressed in this report.

5.5 The United States (US) Report necessarily addresses concern in the US with reference to US law and statute and to US intelligence and law enforcement agencies. It is clear that the relevant circumstances in the US are substantially different from those in the United Kingdom. Unsurprisingly, the broad approach to safeguarding freedom and privacy in a democratic society, and at the same time protecting national security and preventing and detecting crime, correspond in each country. But the detailed manifestation and application of these broad requirements diverge, such that it is not appropriate to extrapolate recommendations from the US report into UK circumstances. This is not to detract in any way from the value and interest of the report: rather to acknowledge that relevant UK questions need to be addressed in a UK context.

5.6 **Sensitivity requirements.** There are, as any reader will understand, unavoidable statutory restrictions on the extent to which I can lawfully publish details in relation to the interception of communications. In particular, I am (with others) subject to the Official Secrets Act 1989 and section 19 of RIPA 2000. Section 19 imposes a duty to keep secret the existence, content and details of interception warrants, everything in intercepted material and related communications data and related matters. Contravention of the statutory provisions is a criminal offence.

5.7 These are restrictions imposed by Parliament. They mean that I am not able to confirm or reject publicly parts of the detail said to derive from Snowden allegations. A reader should not draw any inference one way or the other in this respect from what I do say. However, as will I trust appear, I am able to address matters of concern in a way which I hope will be helpful.

5.8 There is not the same specific statutory restriction in relation to communications data, although I must be careful not to publish matters whose disclosure would be contrary to the public interest.

5.9 The findings of my investigations into the subject matter of these disclosures are detailed throughout this report. I consider a number of publicly expressed questions of concern in so far as they relate to RIPA 2000 Part I matters in the following section of this report.

Section 6
Questions of Concern

In this section I seek to consider some of the legitimate questions raised in relevant public debate which fall within my statutory review responsibility. Some of this will repeat information I have already provided earlier in this report, but I hope that this will for completeness assist the reader.

1. Does the Interception of Communications Commissioner have full access to all information from the public authorities sufficient for him to be able to undertake his statutory functions?[5]

6.1.1 Yes. All those engaged in RIPA 2000 Part I matters have a statutory obligation to disclose and provide to me all such documents and information as I may require for the purpose of enabling me to carry out my statutory functions (section 58(1) – see also section 18(9)).

6.1.2 This means that I have unrestricted access to full information, however sensitive, about the activities I am required to review. I can report that I am in practice given such unrestricted access and that all of my requests (of which there have been many) for information and access to material or systems are responded to in full. I have encountered no difficulty from any public authority or person in finding out anything that I consider to be needed to enable me to perform my statutory functions. On the contrary, the public authorities are keen that I should fully understand what I consider I need to know. They frequently volunteer information which they consider I ought to know or which they think would be useful.

2. Does the Interception of Communications Commissioner have sufficient resources to perform his statutory functions fully? And does he do so sufficiently for public purposes?

6.2.1 Under Section 57(7) of RIPA 2000, the Secretary of State is obliged to consult with me and to make such technical facilities available to me and, subject to Treasury approval as to numbers, to provide me with such staff as are sufficient to ensure that I am able properly to carry out my functions. Subject to practicalities, I have encountered no difficulty in securing agreement to the provision of some necessary additional resources, although at the time of writing, I await progress on others.

6.2.2 **The IOCCO staff and office**. My office now comprises the Chief Inspector, 8 Inspectors and 2 office staff. Details of our budget and expenditure are given in Annex C. There was a temporary reduction in the number of communications data and prison inspections undertaken during the second part of 2013, because one inspector retired during the year and the additional inspectors – see below – were not recruited or fully trained until later in the year.

5 See House of Commons Hansard Debates for 31 October 2013 at Column 380WH

6.2.3 Additional inspectors. Soon after I was appointed, I reviewed how my office was set up, how it worked and how we carried out our inspections. The Joint Parliamentary Committee which scrutinized the then proposed draft Communications Data Bill[6] also recommended that my office should inspect the public authorities that acquire larger volumes of communications data at least annually. As a result, I decided it was necessary to increase the number of inspectors from 5 to 8. Three additional inspectors have been recruited and are now in post, having undertaken the necessary training. We moved to annual inspections from January 2014.

6.2.4 Communications data and prison resources. The staff resources now available to me for communications data and prison inspection purposes are sufficient to enable me to carry out my functions properly in those respects. The inspectors are independent, highly skilled and experienced in the principles and detail of the acquisition and disclosure of communications data and in interception of communications in prisons.

6.2.5 The inspectors have been recruited from a wide variety of backgrounds, and bring with them a broad range of experience working with police forces, law enforcement agencies, industry regulators, universities and telecommunications related private organisations. Their experience covers everything from analytical expertise, criminal and counter-terrorism investigations, forensic telecommunications, to training and lecturing in both the technical and legislative aspects of communications data and covert investigations and acting as accredited SPoCs, SROs and DPs.

6.2.6 They report in writing on each individual inspection and I read and comment on all these reports. The reports systematically address the requirements of the statute, the Code of Practice or relevant prison service policy and make detailed recommendations where the inspections reveal non-compliance. The system and inspections are covered in more detail in Sections 4 and 7 of this report.

6.2.7 Interception of communications resources. I have concluded that to undertake my present statutory functions properly, I need one additional inspector with appropriate technical experience. Steps are being taken to recruit such a person.

6.2.8 There are also certain respects in which the accommodation and technical facilities available to me are not yet sufficient or appropriate. I consider that a team of 8 communications data and prison inspectors and 3 interception inspectors (the Chief Inspector, the additional inspector and myself), can properly undertake the interception inspections and the other related work we currently do provided that we have accommodation and technical facilities which enable us to work efficiently and without interruption. The situation at present does not allow us to do so. For example, sensitive systems to which we need access are housed in another part of the building; there is insufficient space in our office for sensitive work to be undertaken efficiently; and access to our office is unnecessarily difficult for our inspectors or others that we need to help us periodically. There is also the fact that, despite being entirely independent, we are

6 Draft Communications Data Bill Session 2012/13 – HL Paper 79, HC 479 recommendation at paragraph 310. See also The Intelligence and Security Committee's report in February 2013 "Access to communications data by the intelligence and security agencies" Cm 8514 at paragraph 71.

accommodated on the Home Office estate, a department we inspect, and this could give the impression that we are not entirely independent. I have raised these matters with the Home Office and have been told they are being addressed, but not yet, so far as I can see, to much effect.

6.2.9 With the additional resources and facilities, I presently consider that I and my office would continue to be able to satisfy myself that the Part I interception and communications data activities of the relevant public authorities are lawful and proportionate or, to any extent that they may not be, to report that to the Prime Minister.

6.2.10 The scale of interception and communications data inspections. The main public authorities who undertake interception activities or communications data acquisition under RIPA 2000 Part I are large organisations. But my relevant responsibility is confined to their interception and communications data activities and I regard that as manageable. Inspections need to look efficiently at the integrity and lawfulness of the system for applying for and granting warrants or requests for communications data and at the systems that are in place to secure compliance with the statutory safeguards. Individual applications and operations need to be looked at to see that they comply with the statutory and Code of Practice requirements. We do this. In addition, this report shows that my interception oversight has not been confined to formal inspections only – see for instance Retention, Storage and Destruction of Intercepted Material (See paragraphs 3.48 to 3.57), and the extensive work we have undertaken to address Questions of Concern.

6.2.11 A broader resources question. There is also a question whether the scale of our current oversight is regarded by others as sufficient for modern purposes in the national interest. That said, I am not myself clear what a significantly enlarged oversight of RIPA 2000 Part I activities might in detail entail.

6.2.12 There is also an important question of personal responsibility. I regard myself as personally responsible for our oversight and I personally undertake an important part of it. Enlarged oversight would certainly bring more people to bear on it, but it would risk bringing about a bureaucratic dilution of responsibility.

3. Is the Interception of Communications Commissioner fully independent of the government and the public authorities?[7]

6.3.1 Yes. I should regard any serious suggestion otherwise as offensive. What follows is not to be regarded as qualification of this unequivocal assertion.

6.3.2 The office of the Interception of Communications Commissioner has existed since the inception of the Interception of Communications Act 1985. Successive Commissioners have always been judges or retired judges of the Court of Appeal or the former Judicial Committee of the House of Lords. Complete independence is a required hallmark of any judge.

7 There have been media suggestions that the oversight regime of GCHQ in particular is light and ineffective, and that I and other commissioners have limited remit and are reluctant to challenge the agencies.

6.3.3 My predecessors' annual reports have generally been in terms which broadly gave a clean bill of health, subject to points of detail, to the relevant activities of the public authorities which were the subject of their review. A sceptical reader might say or think - and some did - that parts of these reports have been bland, uncritical and lacking in corroborative detail. I have attempted to give in this report as much relevant detail as statutory constraints permit. It is for others to judge the extent to which this is sufficient for public purposes. The investigations which have supported this report have been thorough and penetrating and I have no hesitation in challenging the public authorities wherever this has been necessary.

6.3.4 This report is entirely and without qualification the product of my own independent judgment. It is based on information obtained independently by me or my office. I do not set out or intend to defend, protect or promote the public authorities. If, in my judgment, any of their activities are unlawful or disproportionate, I am obliged to say so in this report and would do so without hesitation. To the extent that this report is in fact supportive, that is because I have been properly satisfied that their activities are lawful and proportionate.

4. Should the Interception of Communications Commissioner be more open in communicating with the public?[8]

6.4.1 I think this is difficult. In the second part of 2013, I declined to make any public comment on Snowden or other matters relating to my statutory functions including a number of requests for media interviews. I detected a degree of frustration in some quarters that I was not prepared to make earlier statements or comments about matters of the kind now contained in this report. The reasons for this were as follows:

6.4.2 **Statutory function.** My statutory function and obligation is to make reports to the Prime Minister. Technically it is his decision what, if any, parts of my report should be published by laying before Parliament. It is difficult, in my view, to publish material which should be in a report to the Prime Minister in advance of such a report.

6.4.3 **Complications and sensitivity.** The whole subject matter with which my office is concerned is complicated and sensitive. Fully understanding it all requires a period of mature experience and reflection, and there was a real risk during the whole of 2013 that I might accidentally and from inexperience overstep the proper limits of sensitivity or make inaccurate or incomplete public statements with off the cuff oral comments.

In addition, investigating a number of aspects of Snowden related matters has required a great deal of substantial work by me, my office and the interception agencies. The product of this appears in this report. There are parts of this report which I could not have written in the summer or autumn of 2013. There are still areas of review that I regard to be work in progress and I will report on these when I have satisfied myself that a full investigation has been completed, and not before.

8 See House of Commons Hansard Debates for 31 October 2013 at Col 380WH.

6.4.4 I trust that, frustrating though the delay may have been for some, this report will cover, so far as I am able, the main matters of public concern.

5. Is RIPA 2000 Part I fit for its required purpose in the developing internet age?[9]

6.5.1 This is a large question. It might be recast as asking whether the internet and technology generally has developed so greatly and rapidly that RIPA 2000 Part I now technically permits the public authorities to intercept communications or acquire communications data in ways which unduly invade the privacy of those who communicate on the internet for entirely legitimate purposes. Even if the public authorities do not in fact unduly invade users' privacy in this way, is there any material risk that they might?

The question requires separate consideration of communications data acquired under Part I Chapter II, interception warrants issued under section 8(1) and section 8(4) of Part I Chapter I.

6.5.2 **General lack of understanding.** Informed public discussion on this topic has been hampered by an entirely understandable general lack of understanding. There is widespread lack of informed understanding of

(a) the structure of the statutory provisions, and

(b) what those concerned with the operation of the statutory provisions actually do.

6.5.3 As to (a), RIPA 2000 Part I contains provisions, some of which are difficult for anyone to get their head round. I will try to help here. Furthermore, I am satisfied that, despite their difficulties, these provisions are properly understood and operated by those who are engaged in their operation. This has included successive Secretaries of State and their relevant officials.

6.5.4 As to (b), there are sensitivity limits to the detail that I can give publicly. But I will be as open as I may. I can be more helpful in explaining what the public authorities do not do. I shall also consider the extent of any risk that the RIPA 2000 safeguards might be wrongfully evaded.

6.5.5 **Historical context.** It is instructive to see the legislation in its historical context and to consider what Parliament contemplated and understood before and during the passage through Parliament of the Bill that became RIPA 2000. It is then appropriate to

9 "Can you see why it is that the public feel that when the last bit of legislation on this was passed in the year 2000 [RIPA 2000] and technology has moved on so fast and your capabilities have developed so hugely, it is hardly credible that the legislation is still fit for purpose for the modern world." Lord Butler of Brockwell questioning the Director General of the Security Service at a session of the Intelligence and Security Committee on 7 November 2013, page 19.

ask what has changed since 2000 to call in question the contemporary integrity of the legislation.

6.5.6 The section 8(4) process in particular was not invented in RIPA 2000. It goes back to the Interception of Communications Act 1985, which already contained in its section 3(2) to (4) and section 6 the essential features of the present section 8(4) structure. The statutory structure has now been in place in its present form for upwards of 13 years.

6.5.7 RIPA 2000 received Royal Assent on 28th July 2000. It is of some relevance to note that this was before the terrorist attack on the Twin Towers in the United States on 11th September 2001. RIPA 2000 was not therefore – as I understand some US legislation was – in reaction to those events.

6.5.8 RIPA 2000 was enacted in part to bring the Interception of Communications Act 1985 up to date so that it should comply with the Human Rights Act 1998.

6.5.9 **Article 8 of the European Convention on Human Rights** provides that –

- "Everyone has the right to respect for his private and family life, his home and his correspondence.
- "There shall be no interference by a public authority with the exercise of the right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedom of others".

6.5.10 I have described the structure of RIPA 2000 Part I for both interception of content and acquiring communications data in Sections 3 and 4 respectively of this report. It will be seen that these structures explicitly embrace the requirements of necessity and proportionality and the exceptionally permitted statutory purposes, all of which derive from Article 8. Thus if conduct under an interception warrant or authority to obtain communications data would disproportionately intrude upon a person's privacy, it would be unlawful to grant the warrant or give the authority. A specific judgment has to be made in this respect by the Secretary of State or the DP for each application.

6.5.11 In short, RIPA 2000 Part I was amending legislation explicitly enacted to protect privacy rights under Article 8 of the European Convention.

Communications data.

6.5.12 The structure of the statutory system for lawfully obtaining communications data under RIPA 2000 Part I Chapter II and the associated Code of Practice is given in Section 4 of this report. It is important that every requirement for communications data has been individually authorised by a process which requires a detailed written application, scrutiny by a SPoC and consideration by an independent DP.

6.5.13 Internal authorisation. An important feature of the system for communications data approval is that, with the exception of those for local authorities which are now authorised by a relevant judicial authority[10], it is internal to the public authority wishing to acquire the communications data. This is in contrast with warrants authorising interception of content which are issued by a Secretary of State. This no doubt is an indication of a parliamentary perception when RIPA 2000 was enacted that intercepting content was potentially more intrusive than acquiring communications data.

6.5.14 A view might be taken that giving authority to acquire communications data internally is unsatisfactory. That view might be strengthened if the inspections which my office undertakes revealed abuse or significant unlawful use of the Part I Chapter II powers. Our inspections do not reveal this. The errors which are reported or uncovered by the inspectors (see paragraphs 4.45 to 4.54) are certainly errors requiring better training or system adjustments in places. But they are numerically very small in relation to the whole and do not significantly detract from the integrity of this part of the statutory scheme.

6.5.15 Safeguards. Safeguards against abuse include:

- the requirement that acquiring communications data must be necessary for one of the Part I Chapter II statutory purposes. Acquiring it for any other purpose would be unlawful;
- the fact that each application has to be made individually in writing and contain written material explaining why each element of the statutory requirements is fulfilled;
- the scrutiny required to be undertaken by the trained SPoCs;
- the consideration required of the (usually independent) DP of the necessity and proportionality of the individual applications;
- the fact that all public authorities which acquire larger volumes of communications data are now inspected annually by our inspectors;
- the fact that we obtain data from CSPs to audit that their disclosures correlate with the public authorities' approvals.

6.5.16 In 2012, there was parliamentary scrutiny of the draft Communications Data Bill by a Joint Committee of both Houses of Parliament and by the Intelligence Services Committee[11]. The Joint Committee considered whether the Part I Chapter II system for acquiring communications data remained appropriate. I understand that, in the early stages of its scrutiny, the Joint Committee (or some of its members) were inclined to think that the system of internal authorisation might no longer be appropriate. However, the Committee's eventual report gave broad approval to the existing statutory system and in particular to the SPoC system[12]. I understand that this change of view (if there was

10 See section 23A of RIPA inserted by amendment by section 37 of the Protection of Freedoms Act 2012.

11 Draft Communications Data Bill Session 2012/13 – HL Paper 79, HC 479; The Intelligence and Security's report in February 2013 "Access to communications data by the intelligence and security agencies" Cm 8514.

12 See paragraph 179 of the Report on the Draft Communications Data Bill (HC/479) "The SPoC system is an

one) resulted in part from a visit by the Committee to the SPoC unit of the Metropolitan Police, when Committee members were able to see how the system works in practice. I have myself visited and inspected the SPoC unit of the Metropolitan Police. I share the Joint Committee's published view as to the integrity of the SPoC system.

6.5.17 Possibility of abuse. It is necessary to consider the possibility of intentional, malign abuse of this Part I Chapter II system resulting in invasion of privacy.

6.5.18 I do not believe that small scale abuse of this kind can be absolutely ruled out. It would probably have to entail a forged application by or with the criminal connivance of an individual SPoC. I do not believe that very small scale abuse of this kind could be guarded against absolutely except conceivably by the installation of very sophisticated protective computer and management systems whose expense would probably not be justified by the risk. A risk of this kind would not be eliminated by changing the authorisation process.

6.5.19 I do not believe that a criminal conspiracy of this kind of any significant scale would happen or go undetected in properly trained professional organisations of palpable integrity with carefully constructed internal processes and safeguards.

6.5.20 Summary. I do not believe that RIPA 2000 Part I Chapter II now permits intrusion into privacy to any greater extent than when the legislation was enacted in 2000. Increases in volume have not affected the integrity of the system. Nor has the increase in volume and sophistication of the internet. Obtaining internet communications data under Chapter II is intrinsically the same operation as obtaining more traditional telephony communications data. The statutory principles remain to be applied in the same way. As has been said, RIPA 2000 is technology neutral.

Section 8(1) Interception Warrants

6.5.21 Procedure for Interception Warrants. This is provided for in sections 5 to 11 of RIPA 2000 Part I Chapter I and the Code of Practice for the Interception of Communications. The essential features of the application process are included in paragraphs 3.11 to 3.21 of this report.

6.5.22 General Safeguards. Section 15 of RIPA 2000 provides for important restrictions on the use of intercepted material. It is an explicit part of my statutory functions under section 57 to keep under review the adequacy of the safeguard arrangements which section 15 imposes on the Secretary of State. This in the main requires a review of the safeguarding procedures which the interception agencies operate.

integral part of the RIPA request process ... It is our view that the SPoC service should be made a statutory requirement for all authorities which have access to communications data."

6.5.23 Dissemination. Section 15(2) in substance requires that the dissemination of intercepted material is limited to the minimum that is necessary for authorised purposes. The authorised purposes are those set out in section 15(4). The main such purpose is that retaining the product of interception continues to be, or is likely to become, necessary for one or more of the original statutory purposes. The restriction on dissemination applies to the number of persons to whom, and the extent to which intercepted material or data is disclosed; the extent to which it is copied and the number of copies made. Copies that are made and retained have to be secure (section 15(5)). These restrictions have to be considered with section 19, which (in very short summary) imposes very strict duties of secrecy about matters relating to interception and provides criminal sanctions for breach of those duties.

6.5.24 These restrictions on dissemination provide a strong protection against any real intrusion into privacy where for instance lawfully intercepted material, unavoidably obtained, is read or listened to by an analyst and immediately discarded as irrelevant.

6.5.25 Destruction. Section 15(3) is important. It provides that each copy made of any intercepted material or related communications data is destroyed no later than when there are no longer grounds for retaining it as necessary for any of the authorised purposes. This has the effect of reducing substantially any risk that the product of interception might be used indiscriminately for anything other than an authorised purpose. The requirement to comply with section 15(3) is at the heart of our Retention, Storage and Destruction investigation described in paragraphs 3.48 to 3.57 of this report.

6.5.26 The section 8(1) element of RIPA 2000 Part I remains, in my view, fit for purpose in the developing internet age. It works just as properly for internet communications where the identifier to be included in the schedule to the warrant is a known internet identifier as it does for more traditional telephony communication.

Section 8(4) Interception warrants

6.5.27 The section 8(4) statutory system has recently given rise to understandable concern.

6.5.28 Statutory structure. It is first necessary to explain the difficult relevant statutory structure. I shall attempt to do this as clearly as I may. For clarity, the forms of expression will in part be mine, not necessarily those in the statute.

6.5.29 Section 8(4) disapplies the provisions of section 8(1) and 8(2) in certain circumstances. This means that a section 8(4) warrant does not have to name or describe one person as the interception subject or a single set of premises as the target of

interception. It does not have to have a schedule setting out specific factors identifying the communications to be intercepted.

6.5.30 The circumstances in which a section 8(4) warrant may be issued are that:

- the communications to be intercepted are limited to *external communications* and their related communications data;
- external communications are communications sent or received outside the British Islands (section 20);
- the warrant may also comprise communications not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises (section 8(5));
- in addition to the warrant, the Secretary of State has to give a *certificate* describing certain of the intercepted material and certifying that the Secretary of State considers that the examination of this described material is necessary for one or more of the statutory purposes (section 8(4)b)), which are;
  - in the interests of national security,
  - for the purpose of preventing or detecting serious crime,
  - for the purpose of safeguarding the economic well-being of the United Kingdom.

6.5.31 The intercepted material which may be *examined* in consequence is limited to that described in a certificate issued by the Secretary of State. The examination has to be certified as necessary for a Part I Chapter I statutory purpose. Examination of material for any other purpose would be unlawful.

6.5.32 Section 15 safeguards apply. The safeguards in section 15 which apply to all interception warrants apply equally to section 8(4) warrants – see paragraphs 6.5.22 to 6.5.25. In particular, section 15(3) requires that each copy of intercepted material and any related communications data is destroyed as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes.

6.5.33 Extra safeguards for section 8(4) warrants. There are extra safeguards in section 16 for section 8(4) warrants and certificates. Parts of section 16 are in convoluted language and style. I will summarise the relevant bits as clearly as I may.

6.5.34 The section 8(4) intercepted material may only be examined to the extent that its examination:

- has been certified as necessary for a Part I Chapter I statutory purpose, and
- does not relate to the content of communications of an individual who is known to be for the time being in the British Islands.

6.5.35 Thus a section 8(4) warrant does not generally permit communications of

someone in the British Islands to be selected for examination. This is, however, qualified to a limited extent by sections 16(3) and 16(5).

6.5.36 Section 16(3) permits the examination of material acquired under a section 8(4) warrant relating to the communications of a person within the British Islands if the Secretary of State has certified for *"the individual in question"* that its examination is necessary for a statutory purposes in relation to a specific period of not more than 6 months for national security purpose or 3 months for serious crime or economic well-being. Since this certificate has to relate to an individual, it is generally equivalent to a section 8(1) warrant.

6.5.37 Section 16(4) and (5) have the effect that material acquired under a section 8(4) warrant for a person who is within the British Islands may be examined for a very short period upon the written authorisation of a senior official where the person was believed to be abroad but it has just been discovered that he or she has in fact entered the British Islands. This will enable a section 8(1) warrant or section 16(3) certificate for that person to be duly applied for without losing what could be essential intelligence.

6.5.38 What this all boils down to is that

- a section 8(4) warrant permits the interception of generally described (but not indiscriminate) external communications.
- this may only be lawfully *examined* if it is within a description certified by the Secretary of State as necessary for a statutory purpose.
- the selection for examination may not be referable to the communications of an individual who is known to be for the time being in the British Islands unless he or she is the subject of an individual authorisation under section 16(3) or (5)[13].
- the section 8(4) structure does not permit random trawling of communications. This would be unlawful. It only permits a search for communications referable to individuals the examination of whose communications are certified as necessary for a statutory purpose.

13 This analysis of what is now section 16 of RIPA 2000 was in substance explained in Parliament during a House of Lords debate on the bill which became RIPA 2000. At that stage, what is now section 16 was clause 15 in the bill. Lord Bassam of Brighton, responding to an opposition amendment (subsequently withdrawn) essentially probing whether clause 8(4) would permit "Orwellian trawling", said at Hansard House of Lords Debates for 12 July 2000 at column 323:
"It is still the intention that Clause 8(4) warrants should be aimed at external communications. Clause 8(5) limits such a warrant to authorising the interception of external communications together with whatever other conduct is necessary to achieve that external interception. Whenever such a warrant is signed, the Secretary of State must be convinced that the conduct it will authorise as a whole is proportionate--my favourite word--to the objects to be achieved. His decision to sign will be overseen by the interception of communications commissioner.
"The next layer of protection is the certificate. Anything that is not within the terms of the certificate may be intercepted but cannot be read, looked at or listened to by any person. Beyond that are the safeguards set out in subsection (2) of Clause 15. Except in the special circumstances set out in later subsections, or if there is an "overlapping" Clause 8(1) warrant, selection may not use factors which are referable to an individual known to be for the time being in the British Islands."

6.5.39 **How section 8(4) is in fact operated**. I have examined in detail the way in which the interception agencies in fact operate under section 8(4) warrants. This is sensitive, but I can give some general indications.

6.5.40 Any significant volume of digital data is literally useless unless its volume is first reduced by filtering. What is filtered out at this stage is immediately discarded and ceases to be available. What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process.

6.5.41 It is a matter of judgment whether a process of this kind has any significant risk of undue invasion of privacy. My own judgment is that it does not, for reasons which I will explain.

6.5.42 If I were to conclude that the section 8(4) procedure is in fact operated unlawfully so as to give rise to improper invasion of privacy, it would unquestionably be my duty to report it to the Prime Minister under section 58(2) of RIPA 2000. I do not so conclude. There are some instances, outlined in the paragraph 3.64 of this report, where the section 16 safeguards have not been fully complied with. These instances do not materially detract from my general conclusion.

6.5.43 The reasons for my judgment that the section 8(4) process does not have a significant risk of undue invasion of privacy are as follows:

- it cannot operate lawfully other than for a statutory purpose. Indiscriminate trawling is not a statutory purpose;
- it cannot operate lawfully other than pursuant to a warrant and one or more certificates issued by the Secretary of State;
- the Secretaries of State who sign warrants and give certificates are well familiar with the process; well able to judge by means of the written applications whether to grant or refuse the necessary permissions; and well supported by experienced senior officials who are independent from the interception agencies making the applications;
- if a warrant is up for renewal, the Secretary of State is informed in writing of the intelligence use the interception warrant has produced in the preceding period. Certificates are regularly reviewed and subject to modification by the Secretary of State;
- examination of intercepted material has to be in accordance with the certificate such that indiscriminate trawling is unlawful;
- with the exception of individuals under section 16(3) (or for very short periods under section 16(5)), examination of intercepted material may not be referable to an individual who is in the British Islands;
- examination of material under section 16(3) referable to the communications

of an individual who is within the British Islands is limited by a process equivalent to that for a section 8(1) warrant;

- the examination of the intercepted material is effected by search criteria constructed to comply with the section 8(4) process;
- the process is subject to Retention, Storage and Destruction policies and procedures which I have examined in detail and which I consider in paragraphs 3.48 to 3.57 of this report.

6.5.44 **Risk of misuse?** It is legitimate to ask what risks are there that this process might miscarry; or what features of it might be seen as unacceptable potential invasion of the privacy of individuals in whom the interception agencies have no legitimate interest. As to which:

- I have personally undertaken a detailed investigation of the statutory, technical and practical operation of section 8(4) warrants;
- I have confirmed that the interception agencies understanding of the relevant statutory and Code of Practice requirements coincides with mine as expressed in this report;
- I have confirmed that the interception agencies technical and practical operation of the section 8(4) process is designed to comply with the statutory and Code of Practice requirements;
- I have also made visits to and had meetings with a number of CSPs to discuss and, so far as I am able, understand the technicalities of their implementation of section 8(4) warrants under section 11 of RIPA 2000. The technicalities are complicated and sophisticated but I believe that I have sufficiently understood their principles at least for present purposes.

Decision of the Investigatory Powers Tribunal about section 8(4).

6.5.45 On 9th December 2004, the Investigatory Powers Tribunal (IPT), in Open Rulings on Preliminary Issues of Law, considered the lawful integrity of section 8(4) of RIPA 2000. I have included an extended summary of these Rulings in Appendix 1 to this report. The general tenor of the Rulings is to endorse the structural integrity in law of the section 8(4) procedure including the principle of a filtering process to reduce and make individual selections from generalised interception material.

6.5.46 In the light of this IPT decision, it is, I think, pertinent to ask what has changed since 2000 or 2004 so that a statutory procedure which was re-enacted in 2000, and whose integrity was judged to be intact in 2004, may now have become inadequate and outdated.

6.5.47 Certainly the use of the internet has expanded in volume and sophistication. Investigatory techniques are no doubt more sophisticated then they were. But I do not

see that either of these by themselves affect the integrity of the statutory structure as supplemented by the Code of Practice.

6.5.48 Privacy and Human Rights. As I have already noted, one of the main reasons for Parliament enacting RIPA 2000 was to make it compliant with the Human Rights Act 1998. Thus RIPA 2000 Part I Chapter I, and the section 8(4) procedures in particular, were enacted as being compliant with the privacy rights in Article 8 of the Convention. There is no reason internal to the statute to suppose that they are any less compliant as statutory provisions now than they were in 2000. No doubt Parliament addressed particular human rights privacy considerations as well in 2000, and it is appropriate to re-address such considerations now with reference to section 8(4).

6.5.49 Since the section 8(4) structure re-enacted in 2000 explicitly enables the generalised initial interception of what at the point of interception is (relatively) unfiltered material, the following questions might arise:

(a) is it in general necessary and proportionate to warrant the initial interception of this kind and volume of material?

(b) are there other reasonable less intrusive means of obtaining the information which it is considered necessary to obtain – this is a consideration which section 5(4) of RIPA 2000 explicitly requires the Secretary of State to take into account?

(c) is there a risk that a process of generalised initial interception would unavoidably also initially intercept some internal communications?

6.5.50 The question at (a) above cannot be properly answered as an isolated question. The necessity and proportionality of the initial interception has to be looked at in the context of:

- what then happens to the interception material;
- to what extent may it be lawfully examined;
- for how long and for what purpose is it retained before being deleted;
- what safeguards are imposed by the statute; and
- are the safeguards adhered to?

I have considered each of these matters in the course of this report.

6.5.51 As to (b) above, I am satisfied that at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure. This is a sensitive matter of considerable technical complexity which I have investigated in detail.

6.5.52 As to (c) above, I am satisfied from extensive practical and technical information provided to me that it is not at the moment technically feasible to intercept external

communications without a risk that some internal communications may also be initially intercepted. This was contemplated and legitimised by section 5(6)(a) of RIPA 2000 which embraces

> *"all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant".*

6.5.53 Thus the unintended but unavoidable initial interception of some internal communications under a section 8(4) warrant is lawful. Reference to Hansard House of Lords Debates for 12th July 2000 shows that this was well appreciated in Parliament when the bill which became RIPA 2000 was going through parliament[14].

6.5.54 However, the extent to which this material, lawfully intercepted, may be lawfully examined is strictly limited by the safeguards in section 16 – see paragraphs 6.5.33 6.5.37 of this report. And in any event my investigations indicate that the volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a section 8(4) warrant.

6.5.55 **Summary.** The upshot of all this is that I do not consider that RIPA 2000 Part I Chapter I, and in particular the section 8(4) process has become unfit for purpose in the developing internet age. There are certainly problems for anyone unfamiliar with the statutory structure in getting a clear understanding of what the statute permits, and conversely what it forbids. There are sensitivity problems which mean that the public cannot (and should not) find out the detail of interception operations which the interception agencies may undertake. But these problems are not new or recent. They have only been highlighted by recent events.

6.5.56 It is ultimately a matter of policy whether the interception agencies, duly authorised under RIPA 2000 Part I Chapter I and subject to its safeguards, should continue to be enabled to intercept external communications, so far as they are lawfully and technically able, in order to assist their functions of protecting the nation and its citizens from terrorist attack, cyber attack, serious crime and so forth. If the policy answer to that question is yes (which I personally should have thought was obvious), the questions then are whether:

---

14 Lord Bassam of Brighton, responding to an opposition amendment (subsequently withdrawn) essentially probing whether clause 8(4) would permit "Orwellian trawling", said at column 323:
"It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious. Noble Lords who have contributed to the debate understand that an internal communication--say, a message from London to Birmingham--may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication."

(a) the present safeguards are sufficient to assure the public that their legitimate privacy is not impaired;
(b) the present structure should be strengthened for the greater protection of privacy.

6.5.57 I leave these questions for others to consider as matters of policy in the light of this report. I would only emphasise here that question (b) above is heavily overlain by matters of sensitive technical possibility, which any changes would need to accommodate.

6.5.58 Furthermore, it is, I believe, beyond question that technological developments relating to the internet may make the public authorities interception and communications data legitimate activities in the public interest more difficult. Recent commentary has tended towards confining the public authorities interception and communications data powers and activities. There is a legitimate policy question whether those capabilities might not need to be enhanced in the national interest. Present public sentiment might not favour that, and changes would obviously need to be very carefully weighed with interests of privacy. But perhaps that policy question should not be completely overlooked.

6. Do the interception agencies misuse their powers under RIPA 2000 Part I Chapter I to engage in random mass intrusion into the private affairs of law abiding UK citizens who have no actual or reasonably suspected involvement in terrorism or serious crime? If the answer to that question is no, is there any material risk that they or somebody might be able to intrude in this way?[15]

6.6.1 I have to a large extent covered this in the previous section of this report.

6.6.2 The answer to the first of the two questions is emphatically no. The interception agencies do not engage in indiscriminate random mass intrusion by misusing their powers under RIPA 2000 Part I. It would be comprehensively unlawful if they did. I should be required to report it to the Prime Minister. I am personally confident from the work I have undertaken throughout 2013 and to date that no such report is required.

6.6.3 In the real world, intrusion in this context into the privacy of innocent persons would require sentient examination of individuals' communications. The legislation only permits this to the extent that it is properly authorised under the statutory structure which I have described and for the necessity purposes which the legislation permits. None of this is 'random' or 'mass' and none of it is directed to intrude into the private affairs of law abiding UK citizens.

15 There have been explicit media suggestions of a surveillance system enabling the state to capture indiscriminately data relating to law abiding citizens; of mass snooping on private communications; of massive unwarranted surveillance that is insecure and unaccountable; and questions whether intrusion only occurs when globally collected data is actually searched.

6.6.4 There will almost always be two parties to a relevant communication. They may perhaps each be properly targeted serious criminals. As often as not, only one of them is, or perhaps neither if, for instance, the communications device is used by others as well as the target. You cannot tell in advance which communications for your serious criminal will be of intelligence interest and which may not. Those which are not may well be theoretically intrusive. Even those which are of intelligence interest may be to an extent intrusive.

6.6.5 It is important that my inspections, and those carried out by our inspectors, look at a sufficient selection of individual applications to see that they are fully and properly drafted and authorised in accordance with the statute and the Code of Practice. This particularly applies to the proportionality sections. But my view, as I have said, is that repetitious inspections of more and more individual applications is eventually less helpful than looking at systems. As to which, there is a number of considerations as follows:

- individual analysts may have to listen to or look at on screen whatever comes before them, be it relevant to an investigation or not. They are experienced and trained to identify quickly and isolate items of legitimate intelligence interest and to deal with them appropriately;
- material which is of no intelligence interest is very quickly passed over, as often as not without being read or listened to. In many systems it is immediately marked for deletion. The deletion will then very soon happen, in many systems automatically;
- meanwhile the analyst, being only human and having a job to do, will have forgotten (if he or she ever took it in) what the irrelevant communication contained. I have sat next to analysts and heard or seen this happening;
- any assessment of the degree of real intrusion should appreciate that this is what inevitably happens on the ground. The active intrusion is insignificant;
- the question never arises, but could in theory be asked, whether it might be an offence under section 19 of RIPA 2000 for an analyst to disclose to anyone the contents of an irrelevant communication marked for deletion;
- deleted material necessarily cannot be searched at all, let alone intrusively;
- conversely it is only stored material that is available for subsequent potential intrusive investigations.

6.6.6 It is for these reasons that I undertook the investigation of the Retention, Storage and Destruction of intercepted material and related communications data in all of the interception agencies with statutory powers to apply for interception warrants under RIPA 2000 Part I Chapter I (See paragraphs 3.48 to 3.57 of this report).

6.6.7 One significant apparent difference between the interception regime under Part I Chapter I and the communications data regime under Part I Chapter II is that there is no explicit statutory destruction provision in Part I Chapter II equivalent to that in section 15(3) for intercepted material. Section 15(3) requires the destruction of intercepted material and related communications data as soon as there are no longer grounds for retaining them as necessary for any of the authorised purposes. I nevertheless take

the provisional view in principle under human rights jurisprudence that communications data should not be held available for any longer period than it is properly required for an authorised statutory purpose.

6.6.8 There have been rumbling publicly expressed undertones that the interception agencies may be operating the section 8(4) interception procedures unlawfully or to the outer limits of legality, so as to produce disproportionate invasion or potential invasion of people's privacy. My clear independent judgment is that this is simply not so, subject to three caveats. Only the third of these should be seen (subject to my further inquiry) as suggesting the possibility of some structural or other reconsideration.

The three caveats are as follows:

(1) my detailed investigation of the Retention, Storage and Destruction of intercepted material and related communications data (See paragraphs 3.48 to 3.57) has unearthed some instances where I conclude further work needs to be done for me to be fully satisfied that some retention periods are not unduly long. This is a general statement referable to several of the interception agencies not specifically directed at the operation of section 8(4) warrants. The proper length of a retention period under section 15(3) – *"as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes"* – is not always clear cut and may be amenable to differing judgments.

(2) the Errors Section of this report has instances where interception has been unintentionally undertaken in error. Every error is regrettable and some of them constitute unintentional unlawfulness. But I consider that the interception errors may properly be seen as largely isolated and fringe problems which, so far as I am aware, have not resulted in any material actual invasion of privacy. [The same is not entirely true of a small handful of communications data errors which are noted in paragraphs 4.51 to 4.53 of this report].

(3) I need to undertake further detailed investigation into the actual application of individual selection criteria from stored selected material initially derived from section 8(4) interception. I have had this fully explained and then demonstrated to me. But I am currently short of sufficient detailed material necessary to make a full structural analysis and assessment of this internal process. Time has not permitted me to undertake this inquiry before writing this report.

6.6.9 My present provisional approach to this last point is as follows:

- individual interception under a section 8(1) warrant is appropriately authorised by a Secretary of State's judgment upon properly structured material;
- the individual acquisition of communications data under RIPA 2000 Part I Chapter II is appropriately authorised by a largely independent DP upon properly structured material. The process is *internal* to the public authority acquiring the data (save for local authorities who must go to a relevant judicial

authority), but is closely prescribed by the Code of Practice;

- the application of individual selection criteria initially derived from a section 8(4) interception warrant is also determined internally to the interception agency by properly structured internal procedures, backed up by independent audit arrangements;
- convinced, as I am, that the main structure for section 8(4) warrants has statutory structural integrity and that it is in fact operated lawfully and so as to avoid disproportionate intrusion into privacy, I nevertheless need to investigate further the breadth and depth of the internal procedures that are being applied to ensure that they are sufficiently strong in all respects.

6.6.10 Risk of unlawful intrusion? The second question under this main heading as to whether there is any real risk that the interception agencies or somebody *might* be able to intrude unlawfully into people's privacy needs further analysis. Conceivably possible candidates for effecting such unlawful intrusion could be:

- the Government;
- one or more of the interception agencies themselves;
- one or more rogue individuals within the interception agencies; or
- by means of aggressive external cyber attack.

6.6.11 The Government. There is, in my judgment, no risk that the Government would or could require the interception agencies to undertake activity which would be unlawful under RIPA 2000 Part I. I ask the question only to dismiss it, but also because I understand that relevant questionable activity may have happened in the United States in the 1970's[16].

6.6.12 Successive Secretaries of State have undertaken their statutory functions of granting warrants under RIPA 2000 Part I Chapter I conscientiously, with complete integrity in the public interest, and without any partisan motive which the lawful subject matter would never embrace anyway.

6.6.13 Secretaries of State do not initiate applications for interception warrants. They respond to applications from the interception agencies which are intended to support their operations. Some of these operations are in general response to intelligence policy priorities of the Joint Intelligence Committee, but these cannot and do not translate into interception applications which are outside the Chapter I statutory necessity purposes.

6.6.14 The Interception Agencies. Unlawful and unwarranted intercept intrusion of any kind, let alone "massive unwarranted surveillance", is not and, in my judgment could not be carried out institutionally within the interception agencies themselves. The interception agencies and all their staff are quite well aware of the lawful limits of their powers. Any form of massive unwarranted intercept intrusion would as a minimum require a significant unlawful internal conspiracy which would never go undetected,

16 See pages 54 to 63 of the Report to President Obama discussed in paragraphs 5.4 and 5.5 of this report.

let alone be concealed from external observation or inspection. It would, for instance, require one or more forged interception warrants or certificates and probably unlawful complicity by CSPs. I reckon that the interception agencies and the CSPs would rightly feel offended that the question needs to be asked.

6.6.15 At a more detailed level, possible unwarranted intrusion cannot happen in the abstract. As I have said, a large body of unfiltered data is useless. An individual or group of individuals cannot possibly have sentient access to a single minute's amount of unfiltered UK communications, let alone communications over any longer period. A progressively selected tiny part of this is needed to make possible any examination by a person upon specific individualised inquiry. This is precisely what sections 8(4) and 16 of RIPA 2000 Part I permit. This, and only this, is what happens.

6.6.16 No one sits in front of a computer screen aimlessly trawling through unselected intercepted material. All searches are for a specific authorised purpose. Any more generic computerised search of stored material for intrusive purposes would be unlawful. But any even theoretical possibility of this is heavily moderated by the facts that:

- such material as is stored is required by section 15(3) to be deleted as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes;
- the filter process necessarily discards large quantities of material which are irrelevant to the interception agencies lawful activities. What remains for any period before it is destroyed is scarcely amenable to mass intrusive surveillance;
- I have carried out the detailed survey of the Retention, Storage and Destruction arrangements of all the interception agencies with powers to apply for interception warrants (see paragraphs 3.48 to 3.57 of this report) with the results which I have described.

6.6.17 A rogue individual or small group. There remains the conceivable, but highly improbable, possibility of small scale unauthorised and unlawful intrusion within the interception agencies by a malign rogue individual or small group. I need to do further detailed research here (see paragraphs 6.6.8 to 6.6.9) and will report in due course, not least to give assurance to the individuals who operate these systems that the work that they do has proper and sufficient protective safeguards.

6.6.18 External cyber attack. This is conceivable, but not within my direct sphere of responsibility or experience. In so far as it might be technically possible - which I simply do not know - I am sure that the interception agencies take proper and appropriate precautions.

7. How can the public feel comfortable in the matter of interception when everything is secret and the public does not know and cannot find out what the interception agencies are doing?

6.7.1 This is an entirely legitimate question. As I have said there are two problems.

6.7.2 First, RIPA 2000 Part I Chapter I is difficult legislation and a reader's eyes glaze over before reaching the end of section 1, that is, if the reader ever starts. The Codes of Practice are more accessible and contain a fairly readable account of the requirements and constraints.

6.7.3 I have given in this report a detailed summary and analysis of the relevant legislation which is intended to be accessible. It sets out to show what the statute permits and what is does not permit. I have tried to be helpful and to set right misunderstandings where I reckon these exist. If the informed public can understand the main shape of the legislation, that should supply part of the comfort. The main shape of the legislation is that it is derived from and fully compliant with Article 8 of the Human Rights Convention; and that interception cannot lawfully take place except by procedures and subject to safeguards designed to achieve that compliance. The starting point is that interception can only be lawfully undertaken for one of the statutory purposes derived from Article 8.

6.7.4 Second, although there is no escaping the statutory constraints on publishing sensitive details about what the interception agencies do in detail, their interception activities are directed, and only directed, in the national interest towards the statutory necessity purposes. I have been able to publish where possible details of what the interception agencies do *not* do, which I hope may help. In the end, there has to be a fair degree of trust, both of the interception agencies themselves, and of the extent to which I and my office are properly able to review the interception agencies RIPA 2000 Part I activities in the public interest.

6.7.5 I am, however, personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant.

8. Do British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes?

6.8.1 No. I have investigated the facts relevant to the allegations that have been published, as to the details of which I am unable to comment publicly. However, the principles that I have applied in reaching this conclusion are as follows.

6.8.2 An intelligence agency in country A is entitled to share intelligence with an intelligence agency in country B if:

(i) the intelligence is lawfully acquired in country A; and

(ii) it is lawful in country A for its intelligence agency to share the intelligence with the intelligence agency in country B; and

(iii) it is lawful in country B for its intelligence agency to receive the intelligence; and for good measure

(iv) it would have been lawful for the intelligence agency in country B to acquire the intelligence in country B, if it had been available for lawful acquisition in that country.

6.8.3 As to (i) and (ii) and generally, I have no expertise in US law and have not personally investigated so much of it as might be relevant. I have however received appropriate assurances in this respect.

6.8.4 As to (ii), if country A is the UK, I have had particular regard to section 15(2) of RIPA 2000 which strictly limits the lawful dissemination of intercept material to the minimum that is necessary for the authorised purposes.

6.8.5 As to (iii), I know of no principle that an intelligence agency is disentitled from receiving intelligence information offered by a third party which a third party lawfully has, provided that its receipt is within the established statutory function of the intelligence agency, as to which see the *Intelligence Services Act 1994*. It happens all the time.

6.8.6 As to (iv), information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to its receipt here even though RIPA 2000 Part I does not strictly apply, because the interception did not take place in the UK by an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies, and I am asked to review the consequent arrangements, although this may not be within my statutory remit.

Points of Note

Questions of Concern

I have full and unrestricted access to all information from public authorities, however sensitive, sufficient for me to be able to undertake my statutory functions.

I am fully independent of the Government and the public authorities which I inspect.

I have (or in one respect soon will have) enough staff to enable me to perform my statutory functions properly, provided that the current accommodation and technical facilities are enhanced in identified respects.

I have considered in detail the large question whether RIPA 2000 Part I remains fit for its required purpose in the developing internet age. I have concluded that it is as fit for purpose as it was when it was enacted. I need to carry out further investigations into one aspect of the operation of Section 8(4).

Public authorities do not misuse their powers under RIPA Part I to engage in random mass intrusion into the private affairs of law abiding UK citizens. It would be comprehensively unlawful if they did. I have considered whether there is a material risk that unlawful intrusion might occur in the operation of Section 8(4). Subject to some further investigation, I conclude there is no material risk.

I am quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant.

British intelligence agencies do not circumvent domestic oversight regimes by receiving from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK.

Section 7
Prisons

7.1 In this section I shall provide an outline of the legislation governing the interception of prisoners' communications, give details of our prison inspection regime and summarise the key findings from our inspections.

Background

7.2 I have continued to provide non-statutory oversight of the interception of communications in prisons in England, Wales and Northern Ireland, as did my predecessors. I do not currently provide any oversight for prisons in Scotland. It would be preferable, in my view, if prison oversight was formalised as a statutory function.

7.3 This non statutory oversight of prisons in England and Wales commenced in 2002 at the request of the then Home Secretary. IOCCO were invited to undertake inspections of the Northern Ireland Prisons by the then Director General of Northern Ireland Prisons in 2008.

7.4 In England and Wales Function 4 of the National Security Framework (NSF) governs the procedures for the interception of prisoners' communications (telephone calls and mail). There are also various Prison Service Instructions (PSIs) (such as 08/2009, 52/2010, 49/2011, 56/2011, 24/2012, 10/2013) that impact on this area. The numerous policy documents are fragmented and contradictory in places and this makes it difficult for the prisons themselves to understand the requirements fully and for our inspectors to conduct the oversight. Our inspectors have, on more than one occasion, come across new PSIs whilst actually inspecting prisons. This is problematic as in these instances we had not had the opportunity to align our inspection baselines to the new policy. Concerns have been raised with the Security Group, National Offender Management Service (NOMS) as to why we were not notified in advance of the implementation dates of PSIs that affect the arrangements for the interception of prisoners' communications.

7.5 NOMS is working towards implementing an Interception PSI and it was our understanding that this PSI would replace all other PSIs. It is not clear whether this is still the intention. In our view it would be very confusing for the establishments who are trying to introduce systems and procedures to comply with the various policies if there are numerous PSIs covering this activity and a lack of clarity over which PSI takes precedence.

7.6 Last year my predecessor reported that NOMS had not formally introduced the interception risk assessment template that was designed in 2011. So far as I am aware, there has again been no progress here. Our inspectors have found themselves in a difficult position whereby they are effectively being asked to promote the use of templates which have not been formally ratified.

7.7 NOMS must get to grips with these issues and put in place a clear defined policy and risk assessment documents for the interception of prisoners' communications.

7.8 With regard to the Northern Ireland prisons it has been accepted practice that where Instructions to Governors are absent or deemed to be out of date the Northern Ireland Prison Service would accept our recommendations based on PSIs issued to establishments in England and Wales. This arrangement is far from ideal and I have recommended that the Northern Ireland Prison Service should be aiming to issue a comprehensive Instruction to Governors to supplement the Northern Ireland Prison Rules in relation to the interception of prisoners' communications.

Authorisations to Intercept Prisoners Communications

7.9 **Necessity.** A Governor may make arrangements to intercept a prisoner's (or class of prisoners) communications if he believes that it is necessary for one of the purposes set out in Prison Rules 35A(4) (or Northern Ireland Prison Service Prison Rules 68A(4)). These are:

- the interests of national security;
- the prevention, detection, investigation or prosecution of crime;
- the interests of public safety;
- securing or maintaining prison security or good order and discipline in prison;
- the protection of health or morals; or
- the protection of the rights and freedoms of any person.

7.10 **Proportionality**. A Governor may only give authority to intercept a prisoner's (or class of prisoners) communications if he believes the conduct authorised is proportionate to what is sought to be achieved by that conduct.

7.11 **Types of monitoring.** Interception is mandatory in some cases, for example, high risk or exceptionally high risk Category A prisoners and prisoners on the Escape list. It is often necessary to monitor prisoners for offence related purposes, for example, those who have been convicted of sexual or harassment offences or who pose a significant risk to children. All other prisoners may be subject to monitoring where the Governor believes that it is necessary and proportionate for one of the purposes set out in Prison Rules. Monitoring is conducted on the basis of an interception risk assessment and an authorisation signed by the Governor.

7.12 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 or a prisoner's constituency MP.

Inspection Regime

7.13 Objectives of Inspections. The primary objectives of our inspections are to ensure that:

- All interception is carried out lawfully and in accordance with the Human Rights Act (HRA) and the Prison Rules made under the Prison Act 1952 or section 13 of the Prison Act (Northern Ireland) 1953;
- All prisons are fully discharging their responsibilities to inform the prisoners that their communications may be subject to interception;
- There is consistency in the approach to interception work in prisons;
- The proper authorisations and risk assessments are in place to support the monitoring of prisoners telephone calls and mail;
- Appropriate measures are being afforded to the retention, storage and destruction of intercept product.

7.14 Number of inspections. The 8 full time inspectors undertake the prison inspections. In 2013 our office conducted 88 prison inspections which equates to approximately two thirds of the establishments.

7.15 The length of each inspection depends on the category and capacity of the prison being inspected. The majority of the inspections take place over 1 day. Inspections of the larger capacity or high security (Category A) prisons may take place over 2 days.

7.16 Examination of systems and procedures for the interception of prisoners' communications. Our prison inspections are structured to ensure that key areas derived from Prison Rules, the relevant PSIs and policies are scrutinised. A typical inspection includes examination of the following areas:

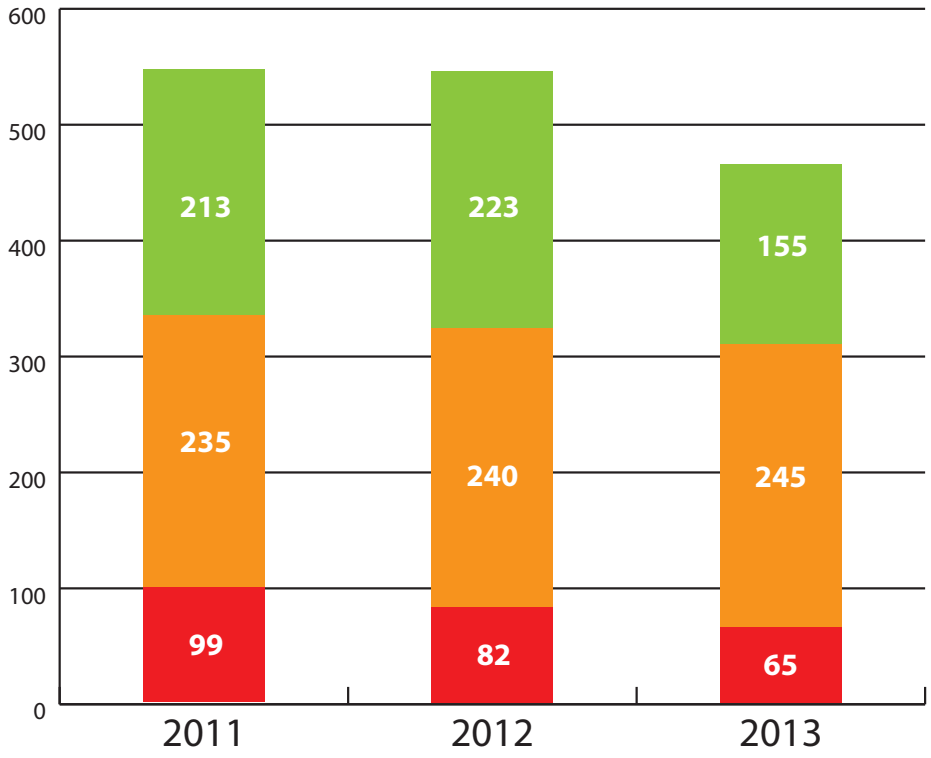
- Induction and awareness of prisoners;
- Procedures for the monitoring prisoners' telephone calls and mail (including risk assessments, authorisations, monitoring logs);
- Arrangements for the handling of legally privileged and other confidential telephone calls and mail;
- Procedures for the storage, retention and destruction of intercept material.

7.17 Inspection Reports. The reports contain a review of compliance against a strict set of baselines that derive from Prison Rules and other policy documents. They contain formal recommendations with a requirement for the prison to report back within two months to say that the recommendations have been implemented, or what progress has been made.

Inspection Findings and Recommendations

7.18 The total number of recommendations made during our 88 prison inspections in 2013 was 465, on average about 5 recommendations for each prison. There has been a marked general improvement in the last three years with inspectors identifying fewer recommendations as exemplified by Figure 12.

Figure 12 *Total red, amber & green recommendations resulting from prison inspections 2011-2013*



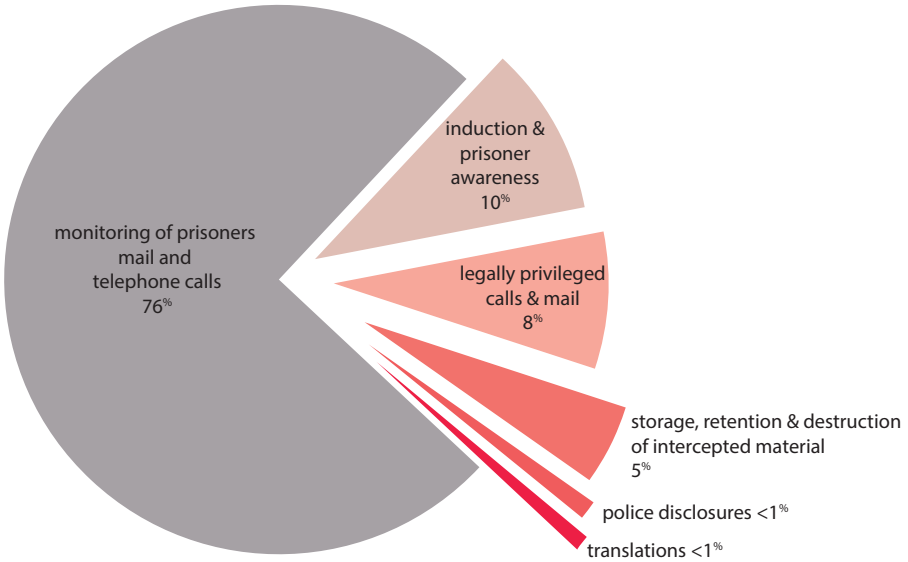
7.19 A traffic light system (red, amber, green) is in place for the recommendations to enable prisons to prioritise the areas where remedial action is necessary:

- Red recommendations - immediate concern - serious breaches and / or non-compliance with Prison Rules or the NSF which could leave the Governor vulnerable to challenge.
- Amber recommendations - non-compliance to a lesser extent; however remedial action must still be taken in these areas as they could potentially lead to serious breaches.
- Green recommendations - represent good practice or areas where the efficiency and effectiveness of the process could be improved.

7.20 This year 14% of the recommendations were red, 53% amber and 33% green.

7.21 Figure 13 shows the breakdown of the 2013 recommendations by category.

Figure 13 *2013 Prison inspection recommendations by Category*



7.22 76% of the recommendations fell into 1 key category – procedures for the monitoring of prisoners telephone calls and mail. There are four distinct areas of failings in this category.

7.23 First, failings were identified with the authorisation and / or review procedures. In a large number of instances our inspectors concluded that the interception risk assessments were not robustly or properly completed. In these instances the necessity and proportionality justifications for invoking or reviewing the monitoring had not been sufficiently made out. In these cases it was difficult to understand how the Governor had been able to make an informed judgement as to whether the monitoring was necessary and proportionate on the basis of the information contained on the risk assessment, authorisation and review documentation. In a number of cases the inspectors examined other relevant documentation in the prisoner's files and / or reviewed the minutes from risk management meetings where the particular prisoner had been discussed in an attempt to satisfy themselves that there was sufficient evidence to support the decisions.

7.24 Second, failings were identified in relation to the actual monitoring. Our inspectors randomly interrogate the system used for the monitoring of prisoners telephone calls and the prisoners accounts are compared against the monitoring logs completed by the

staff conducting the monitoring. In some instances these audits showed that not all of the calls made by the prisoners subject to offence related or monitoring for other security purposes had been listened to. Failure to monitor the communications of prisoners who pose a risk to children, the public or the good order, security and discipline of the prison could place prison staff in an indefensible position if a serious incident was to occur which could have been prevented through the gathering of intercept intelligence. More frequently our inspectors identified that the calls had been listened to, but not in a timely fashion. This is of concern and could result in a significant piece of intelligence being gathered from a telephone call which was made a week or two earlier and by this time the opportunity to react to it may have been missed. It is vitally important for calls to be monitored in a timely fashion in order to evaluate properly the threat posed by prisoners.

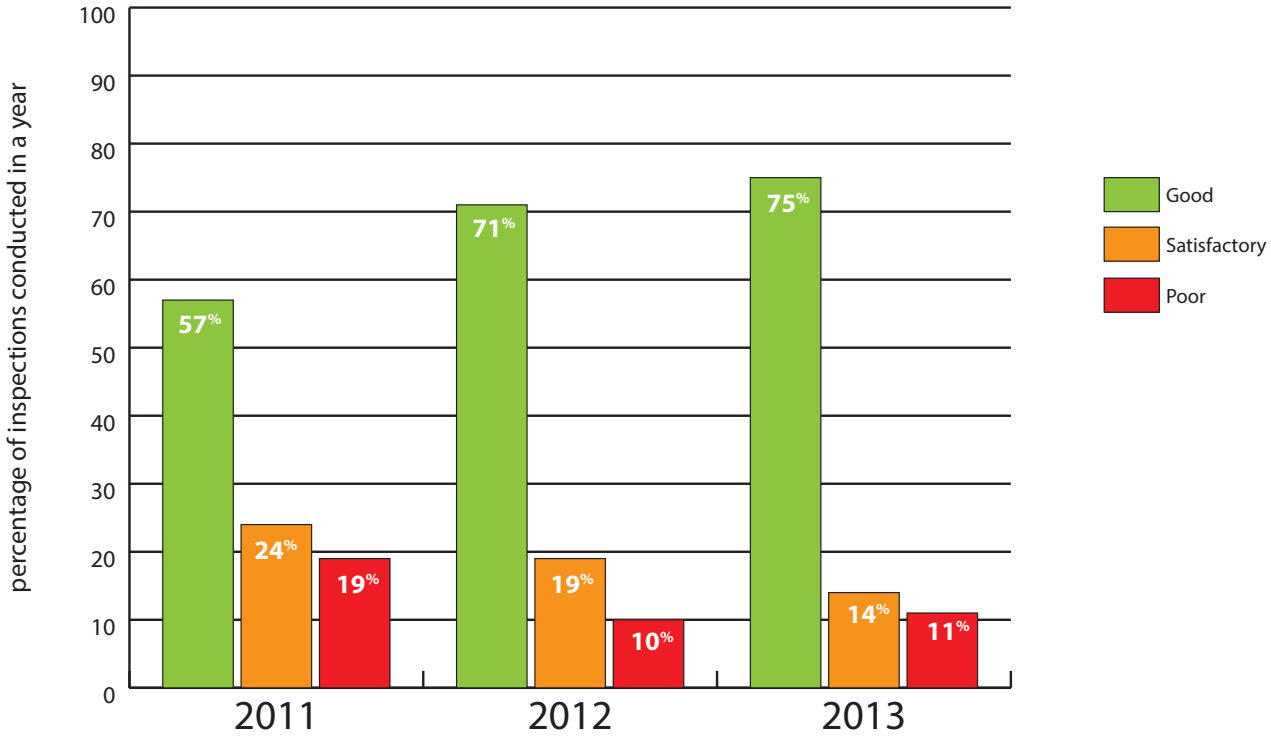
7.25 Third, the staff conducting the monitoring of prisoners communications should complete monitoring logs to provide an audit trail of the interception that has taken place and assist to inform the review process. In a large number of cases the monitoring logs were not completed to a satisfactory standard and recommendations were made to bring about improvements.

7.26 Fourth, failings were identified with the procedures in place for checking the contact numbers provided by prisoners subject to public protection measures (for example, those identified as posing a risk to children, those remanded or convicted of an offence under the Protection from Harassment Act or subject to a restraining order or injunction etc.). In the majority of cases the failings were in relation to the record keeping requirements. However, of more concern, a number of the establishments did not have robust procedures for checking these prisoners contact numbers. It is obviously vitally important for sound procedures to be in place to check the contact lists provided by these prisoners to ensure that victims and other members of the public are protected.

7.27 At the end of each inspection, each individual prison is given an overall rating (good, satisfactory, poor). This rating is reached by considering the total number of recommendations made, the severity of those recommendations, and whether those recommendations had to be carried forward because they were not achieved from the previous inspection. On the latter point, 94% of the prisons inspected in 2013 had fully achieved all or the majority of the recommendations emanating from their previous inspection.

7.28 Figure 14 shows that overall the proportion of prisons achieving a good level of compliance has steadily risen in the last three years. Comparisons with previous years are difficult because the prisons being inspected are not the same. However the average number of recommendations per inspection has fallen slightly in the last 3 years.

Figure 14 *Overall rating for prison inspections 2011-2013*



Points of Note

Prisons

I have continued to provide non-statutory oversight of the interception of communications in prisons in England, Wales and Northern Ireland. I do not currently provide any oversight for prisons in Scotland. It would be preferable, in my view, if prison oversight was formalised as a statutory function.

The policy covering the interception of prisoners' communications in England and Wales is fragmented and contradictory in places. This makes it difficult for the prisons themselves to understand the requirements fully and for our inspectors to conduct the oversight. NOMS must put in place a clear defined policy and risk assessment documents for the interception of prisoners' communications.

I have recommended that the Northern Ireland Prison Service should be aiming to issue a comprehensive Instruction to Governors to supplement the Northern Ireland Prison Rules in relation to the interception of prisoners' communications.

In 2013 our office conducted 88 prison inspections which equates to approximately two thirds of the establishments.

A total of 465 recommendations emanated from these inspections, on average about 5 recommendations for each prison. There has been a marked general improvement in the last three years with inspectors identifying fewer recommendations. Overall the proportion of prisons achieving a good level of compliance has steadily risen in the last three years.

Appendix 1: Decision of the Investigatory Powers Tribunal about section 8(4) of RIPA 2000

The Investigatory Powers Tribunal (IPT) is a tribunal established by section 65 of RIPA 2000. It is the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 for proceedings under section 7(1)(a) of the 1998 Act against any of the intelligence services (see section 65(2)(a) and (3) of RIPA 2000). There is no appeal against determinations of the Tribunal and their decisions may not be questioned in any court (section 67(8)). Their decisions may be regarded in effect as binding authority.

The Interception of Communications Commissioner has no function in relation to the Tribunal and is not made aware of any of their unpublished deliberations, except that, by section 57(3) of RIPA 2000, the Commissioner is obliged to give the Tribunal all such assistance as the Tribunal may require for their investigations or determinations. I personally have not been asked so far to assist the Tribunal and I am not aware that my predecessors have been asked in the recent past.

Decision (IPT/01/77). On 9th December 2004, in Open Rulings on a Preliminary Issues of Law, the Tribunal considered the lawful integrity of section 8(4) of RIPA 2000. Eventually, the Tribunal considered and determined one issue only. But it is evident from the decision that the complainants, who were represented by leading counsel, had initially raised (but abandoned) other issues. I do not know (other than by possible inference) what those other issues were, nor do I have access to the underlying facts which were alleged. But I imagine that leading counsel would have been instructed to pursue other issues if it had been thought that they were viable.

The issue which the Tribunal did examine was

"... the lawfulness of the "filtering process" relating to material obtained pursuant to a warrant issued under section 8(4) of [RIPA 2000]." (paragraph 4 of the Ruling).

The challenge was that there were no published selection criteria for the operation of a section 8(4) warrant and that the section 8(4) process was therefore not "in accordance with law" for the purpose of Article 8 of the Human Rights Convention.

The Tribunal rejected this contention with detailed reference to a number of cases containing relevant human rights jurisprudence. They accepted the case advanced on behalf of the respondents (the three Intelligence Services) that

"the scope and manner of exercise of the powers to intercept communications and make use of the information obtained are indicated with a requisite degree of certainty to satisfy the minimum requirements ... " Christie v United Kingdom [1993] 78-ADR 119 at 133ff.

The respondent's submissions proceeded

"... by reference to the criteria in section 5(3), as exercised with proportionality and the existence of the multiple safeguards". (Rulings paragraph 38).

The final paragraph 39 of the Rulings is as follows:

"The provisions, in this case the right to intercept and access material covered by a s8(4) warrant, and the criteria by reference to which it is exercised, are in our judgment sufficiently accessible and foreseeable to be in accordance with the law. The parameters in which the discretion to conduct interception is carried on, by reference to s5(3) and subject to the safeguards referred to, are plain from the face of the statute. In this difficult and perilous area of national security, taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed on the Respondent, we are satisfied that the balance is properly struck".

This ruling is, so far as it goes, in the nature of binding authority, at least so long as the Tribunal does not depart from it or modulate it. I say "so far as it goes", because on a narrow view the Tribunal only decided one issue. It might be possible for a different legal challenge to be advanced, although, as I have indicated, other issues were advanced in this case but abandoned. The general tenor of the Rulings is to endorse the structural integrity in law of the section 8(4) procedure including the principle of a filtering process to reduce and make individual selections from generalised interception material.

In the course of the Ruling, the Tribunal considered and took account of the following:

the relevant provisions of Article 8 of the Human Rights Convention; sections 5, 8(1), 8(4), 8(5), 15(1),(2) and (3) and 16 of RIPA 2000; and paragraphs 4.2, 4.8 and 5.2 of the Code of Practice;

no challenge was made to the lawfulness of the procedures under a section 8(1) warrant (paragraph 10);

no challenge was made to the lawfulness of a section 8(4) warrant itself nor to the interception of material pursuant to such warrant (paragraph 10);

the Tribunal's own view that there is no difference in the access provisions for section 8(1) and section 8(4) warrants (paragraphs 20.3 and 22);

parts of a witness statement from a Director General at the Home Office referring to public authority manuals setting out comprehensive instructions for the specific application of section 15 and 16 safeguards (paragraph 14); and the process under section 8(4) permitting the selection and examination of selected material within the statutory limits and safeguards (paragraph 33).

Annex A: Public Authorities with access to Communications Data under RIPA Part I Chapter II

Public Authority Group	Data Type (RIPA s.21(4))			Statutory Purpose (RIPA s.22(2) & SI 2010/480)									
	Traffic	Service Use	Subscriber	(a) national security	(b) prevent detect crime / prevent disorder	(c) economic well being of the UK	(d) – public safety	(e) – public health	(f) tax, duty, levy...	(g) in an emergency preventing death / injury...	Art 2(a) miscarriage of justice	Art 2(b) to identify person who has died or is unable to identify themselves, to identify next of kin or other person	Notes
- Intelligence Services	•	•	•	•	•	•							
- Territorial Police Forces of England, Wales, Northern Ireland & Scotland - British Transport Police	•	•	•	•	•	•	•	•		•		•	(d) & (e) subscriber only
- National Crime Agency	•	•	•		•					•		•	
- The Commissioners for Her Majesty's Revenue and Customs	•	•	•		•				•				(f) subscriber only
- United Kingdom Border Agency	•	•	•		•		•					•	(d) subscriber only. Asylum fraud investigations can only acquire service use and subscriber information.
- Ministry of Defence Police - Royal Air Force Police - Royal Military Police - Royal Naval Police	•	•	•	•	•	•				•			
- Civil Nuclear Constabulary	•	•	•	•	•								
- Port of Dover Police - Port of Liverpool Police	•	•	•		•		•	•				•	(d) & (e) subscriber only
- Financial Conduct Authority - Gambling Commission - Gangmasters Licensing Authority - The Information Commissioner - Office of Communications - Police Ombudsman for Northern Ireland - Royal Mail Group - Serious Fraud Office	•	•	•		•								
- Independent Police Complaints Commission	•	•	•		•							•	

- The Ministry of Justice - National Offender Management Service - Northern Ireland Office - Northern Ireland Prison Service	•	•	•	•		•					•	(d) subscriber only
- Criminal Cases Review Commission - Scottish Criminal Cases Review Commission	•	•	•							•		
Department of Transport: - Air Accident Investigation Branch - Marine Accident Investigation Branch - Rail Accident Investigation Branch	•	•	•			•						
- Department for Transport Maritime Coastguard Agency - Fire & Rescue Authorities - Ambulance Services / Trusts	•	•	•	•		•			•			(b) service use & sub-scriber only (d) subscriber only. (g) traffic, service use & subscriber
- Environment Agency - Health & Safety Executive - Department for Health - Medicines & Healthcare Products Regulatory Agency - Scottish Environment Protection Agency		•	•	•		•	•					(d) & (e) subscriber only
- Food Standards Agency		•	•	•			•					(e) subscriber only
- Charity Commission - DWP – Child Maintenance Group - Department of Agriculture & Rural Development (Northern Ireland) - Department for Business Innovation Skills - Department for Environment Food & Rural Affairs - Department of the Environment Northern Ireland - Health & Social Care Business Services Organisation - Central Services Agency (Northern Ireland) - Office of Fair Trading - Pensions Regulator - NHS Protect - NHS Scotland Counter Fraud Services - The Department of Enterprise Trade and Investment (orthern Ireland)		•	•	•								
- Local Authorities		•	•	•			•					

Annex B: Total Notices & Authorisations for each Public Authority under RIPA 2000 Part I Chapter II

This Annex details the Total RIPA 2000 s.23(3) Authorisations granted or s.22(4) Notices given during 2013 by individual Public Authorities, excluding those given orally in urgent circumstances. It is organised according to public authority type*.

A Total of 514,608 Notices and Authorisations (excluding urgent oral) were granted /given under RIPA 2000 Part I Chapter II by 214 public authorities in 2013.

***Caveat:** The main report (paragraphs 4.18 and 4.19) has highlighted the fact that the statistics we are currently able to collect under Paragraph 6.5 of the Communications Data Code of Practice are flawed and potentially misleading. This annex details the number of Authorisations granted and Notices given for communications data by individual public authorities. Authorisations and Notices are the method by which public authorities make requests for communications data. There are essentially 2 difficulties with the Authorisation and Notice Statistics:*

- *Some public authorities may request multiple items of data on one authorisation or notice*
- *There are a number of different workflow systems in use by public authorities which have different counting mechanisms for authorisations and notices.*

The inconsistent counting and aggregation of data requests on a single authorisation and notice mean that the statistics, although accurately recorded by each individual public authority, are not necessarily comparable

Police Forces & Law Enforcement Agencies

	Total
Avon & Somerset Constabulary	9,868
Bedfordshire Police	2,743
British Transport Police	1,260
Cambridgeshire Constabulary	2,166
Cheshire Constabulary	3,814
City of London Police	2,587
Civil Nuclear Constabulary	11
Cleveland Police	2,957
Cumbria Constabulary	2,710
Derbyshire Constabulary	2,897
Devon & Cornwall Police	11,471
Dorset Police	4,316
Durham Constabulary	6,218
Dyfed Powys Police	2,266
Gloucestershire Constabulary	1,590
Greater Manchester Police	19,247
Gwent Police	2,460
Hampshire Constabulary	8,818
Hertfordshire Constabulary	7,567
HMRC	11,820
Humberside Police	2,123
Kent Police & Essex Police	16,242
Lancashire Constabulary	10,690
Leicestershire Police	5,697
Lincolnshire Police	1,734
Merseyside Police	22,347
Metropolitan Police	94,778

	Total
Ministry of Defence Police	171
National Crime Agency	40,064
Norfolk Constabulary	1,923
North Wales Police	2,037
North Yorkshire Police	4,058
Northamptonshire Police	2,169
Northumbria Police	6,211
Nottinghamshire Police	7,749
Police Scotland	19,390
Police Service of Northern Ireland	6,395
Port of Liverpool Police	12
Royal Air Force Police	20
Royal Military Police	706
Royal Navy Police	16
South Wales Police	8,777
South Yorkshire Police	6,801
Staffordshire Police	5,121
Suffolk Constabulary	1,247
Surrey Police	5,193
Sussex Police	3,051
Thames Valley Police	5,221
UK Border Agency	6,056
Warwickshire Police	1,076
West Mercia Police	10,816
West Midlands Police	28,254
West Yorkshire Police	12,676
Wiltshire Police	5,636

Grand Total	451,243

The Port of Dover Police reported that they did not grant any Authorisations or give any Notices in 2013

The Intelligence Services

	Total
GCHQ	1,406
The Secret Intelligence Service (Mi6)	672
The Security Service (Mi5)	56,918
Grand Total	58,996

Other Public Authorities

	Total
Air Accident Investigation Branch	4
Criminal Cases Review Commission	2
Department for Business, Innovations & Skills	34
Department of Enterprise Trade & Investment (Northern Ireland)	118
Department of the Environment Northern Ireland	1
Department of Work & Pensions Child Maintenance Group	29
Environment Agency	18
Financial Conduct Authority	1618
Gambling Commission	16
Gangmasters Licensing Authority	50
Hampshire Fire & Rescue Service	2
Health & Safety Executive	15

	Total
Independent Police Complaints Commission	50
Information Commissioner's Office	40
Marine Accident Investigation Branch	11
Maritime & Coastguard Agency	2
Medicines and Healthcare Products Regulatory Agency	105
Ministry of Justice - National Offender Management Service	267
NHS Protect	21
NHS Scotland Counter Fraud Services	3
Office of Communications	39
Office of Fair Trading	3
Rail Accident Investigation Branch	2
Royal Mail	119
Serious Fraud Office	34
Grand Total	2,603

The following 'other' public authorities reported that they did not grant any Authorisations or give any Notices during 2013:

- Charity Commission
- Department for Environment, Food and Rural Affairs
- Department of Agriculture and Rural Development Northern Ireland
- Food Standards Authority
- Health & Social Care Business Services Organisation - Central Services Agency (Northern Ireland)
- Northern Ireland Office - Northern Ireland Prison Service
- Northern Ireland Health & Social Services Central Services Agency
- The Office of the Police Ombudsman for Northern Ireland
- Pensions Regulator
- Scottish Criminal Cases Review Commission
- Scottish Environmental Protection Agency
- No other Fire Authority
- No Ambulance Service / Trust

Local Authorities

121 Local Authorities have reported never using their powers to acquire communications data

172 Local Authorities in England, Wales, Scotland and Northern Ireland reported they did not use their powers in 2013, but have used their powers in previous years.

The following 132 Local Authorities reported using their powers in 2013

	Total
Aberdeenshire Council	4
Argyll and Bute Council	4
Bedford Borough Council	10
Birmingham City Council	87
Blackburn with Darwen Borough Council	2
Blackpool Borough Council	6
Bournemouth Borough Council	13
Bracknell Forest Borough Council	3
Bridgend County Borough Council	6
Brighton & Hove City Council	2
Bristol City Council	12
Buckinghamshire County Council	79
Bury Metropolitan Borough Council	4
Caerphilly County Borough Council	5
Cannock Chase Council	1
Cardiff City and County Council	3
Central Bedfordshire Council	1
Cheshire East Council	63
Cheshire West & Chester Council	75
Cornwall County Council	17
Cotswold District Council	1
Coventry City Council	7
Cumbria County Council	3
Darlington Borough Council	9
Denbighshire County Council	13
Derbyshire County Council	3
Devon County Council	2
Doncaster Metropolitan Borough Council	2
Dorset County Council	6
Dudley Metropolitan Borough Council	4
Dundee City Council	1
Durham County Council	4
East Ayreshire District Council	2

	Total
East Hertfordshire District Council	7
East Riding of Yorkshire Council	3
East Sussex County Council	12
Edinburgh City Council	4
Fife Council	1
Flintshire County Council	4
Gateshead Metropolitan Borough Council	1
Glasgow City Council	21
Gloucestershire County Council	7
Hampshire County Council	12
Hertfordshire County Council	6
Hertsmere Borough Council	12
Kent County Council	50
Knowsley Metropolitan Borough Council	24
Lancashire County Council	37
Leicester City Council	3
Lincolnshire County Council	26
Liverpool City Council	28
London Borough of Barnet Council	6
London Borough of Brent Council	2
London Borough of Bromley Council	87
London Borough of Croydon Council	9
London Borough of Ealing Council	2
London Borough of Enfield Council	87
London Borough of Hammersmith & Fulham	2
London Borough of Havering Council	22
London Borough of Lambeth Council	2
London Borough of Lewisham Council	4
London Borough of Merton	2
London Borough of Newham Council	4
London Borough of Redbridge	21
London Borough of Richmond upon Thames	1
London Borough of Southwark	4

Local Authorities continued...

	Total
London Borough of Sutton	11
London Borough of Tower Hamlets	25
Manchester City Council	4
Medway Council	5
Middlesborough Council	19
Milton Keynes Council	17
Monmouthshire County Council	1
Neath Port Talbot County Borough Council	4
Newport City Council	2
Norfolk County Council	2
North East Lincolnshire Council	4
North Kesteven District Council	1
North Lanarkshire Council	18
North Lincolnshire Council	6
North Yorkshire County Council	7
Northamptonshire County Council	31
Northumberland County Council	3
Nottingham City Council	1
Nottinghamshire County Council	58
Oldham Metropolitan Borough Council	7
Oxfordshire County Council	10
Peterborough City Council	1
Plymouth City Council	7
Poole Borough Council	6
Portsmouth City Council	1
Reading Borough Council	4
Redcar & Cleveland Borough Council	69
Rhondda Cynon Taff County Borough Council	11
Rochdale Metropolitan Borough Council	6
Rotherham Borough Council	2
Royal Borough of Greenwich Council	1
Royal Borough of Kingston upon Thames Council	1
Royal Borough of Windsor and Maidenhead	10

	Total
Rushmoor District Council	1
Sandwell Metropolitan Borough Council	6
Slough Borough Council	20
Solihull Metropolitan Borough Council	7
South Oxfordshire District Council	4
South Somerset District Council	2
Southampton City Council	81
St Helens Metropolitan Borough Council	3
Staffordshire County Council	3
Stirling Council	5
Stockton-on-Tees Borough Council	2
Stoke-on-Trent City Council	2
Suffolk County Council	21
Surrey County Council	1
Swale Borough Council	1
Swansea City and County Council	5
Swindon Borough Council	9
Tameside Metropolitan Borough Council	2
Three Rivers District Council	4
Torbay Borough Council	1
Vale of White Horse District Council	2
Walsall Metropolitan Borough Council	3
Warrington Council	15
Watford Borough Council	53
Wealden District Council	3
West Berkshire Council	31
West Sussex County Council	22
Westminster City Council	31
Wigan Metropolitan Borough Council	2
Wirral Metropolitan Borough Council	1
Wolverhampton City Council	6
Worcestershire Regulatory Services*	15
York City Council	80

Grand Total	1766

*Worcestershire Regulatory Services is a shared service acting on behalf Worcestershire County Council, Redditch Borough Council, Bromsgrove District Council, Wyre Forest District Council, Worcester City Council, Malvern Hills District Council and Wychavon District Council.

Annex C: Budget

Our office had a budget for 2013/14 of **£1,101,000** allocated as below.

Expenditure for 2013/14 was not available at the time of going to print but will be available on our website after the end of April 2014.

I am aware the salary, travel and subsistence costs will be significantly less than the budget due to the timing of the recruitment of the 3 new inspectors.

Descripton	Total (£)
Staff costs	948,000
Travel and subsistence	110,000
IT and telecommunications	25,000
Training & recruitment	5,000
Office and security equipment	3,500
Conferences and meetings	7,000
Legal	2,500

ISBN 978-1-4741-0157-8