Report of the Interception of Communications Commissioner

March 2015

(covering the period January to December 2014)

The Rt Hon.
Sir Anthony May

Report of the Interception of Communications Commissioner

March 2015

(covering the period January to December 2014)

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 12th March 2015

Laid before the Scottish Parliament by the Scottish Ministers 12th March 2015

HC 1113

SG/2015/28

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 9781474116251

Web ISBN 9781474116268

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

ID 05031502 03/15

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

March 2015

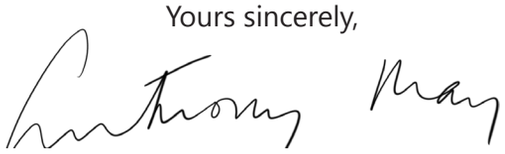
Dear Prime Minister,

I am required by section 58(4) of the Regulation of Investigatory Powers Act (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 half year. This report covers the calendar year of 2014 and from this point forward I will be reporting half-yearly.

I was delighted to return to my role as Interception of Communications Commissioner on 1st January 2015 in time to prepare this report. I would like to thank the Rt Hon. Sir Paul Kennedy and all the members of my office for their unwavering support and for the considerable work they undertook during my absence in the second part of the reporting year.

You are required to lay a copy of my half-yearly reports before each House of Parliament (section 58(6)) together with a statement as to whether any matter has been excluded 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 again 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 is my second report as Interception of Communications Commissioner. My 2013 report was well received and I have therefore retained the form and some of the legislative background and explanatory content this year.

1.2 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 the Regulation of Investigatory Powers Act 2000 (RIPA 2000) Part I (and to a limited extent Part III) do so lawfully and in accordance with the existing legislation. My secondary, but nonetheless important, aim is to better inform the public about what the legislation allows (or perhaps more importantly what it does not allow), how my office carries out its oversight and the level of compliance that the public authorities are achieving.

1.3 It is perhaps useful to revisit the role that Parliament intended the Interception of Communications Commissioner to carry out when the RIP Bill was debated in 2000. It is clear from the debates that the intention was for the Commissioner to *"conduct audits and check what is happening in practice, rather than examine every case universally"*[1]. I am satisfied that my office has introduced a vigorous audit and inspection regime to enable us to carry out the function intended by Parliament effectively. It was recently said that the Interception of Communications Commissioner *"acts like a public conscience, identifying when RIPA 2000 is not used as expected"*[2] and this portrayal of my role is particularly relevant to some of the investigations and inquiries that my office has undertaken recently.

1.4 I do not regard myself as a promoter of the legislation or of the public authorities' use of it. My primary focus is to audit independently compliance against existing legislation. Changes to the legislation and matters of policy are for others, Parliament in particular, to consider and decide. The Investigatory Powers Tribunal (IPT) also has an exclusive role in the United Kingdom in proceedings for actions that are incompatible with the European Convention on Human Rights (ECHR).

1.5 I again make the point that it is a challenge to provide a full public account of what the intelligence agencies in particular actually do because much of the operational detail is sensitive for understandable reasons. Furthermore with regard to the interception of communications my office is constrained by the statutory provisions in section 19 of RIPA 2000 forbidding disclosure, as are the interception agencies and Communication Service Providers (CSPs). For these reasons there is always going to be certain information that I cannot reveal publicly, but this limit to transparency certainly does not mean that there is limited accountability.

1.6 I can report that I have full and unrestricted access to all of the information and material that I require, however sensitive, to undertake my review. I am in practice given such unrestricted access and 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

1 Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill Comments by the Minister of State, Home Office (Mr. Charles Clarke)

2 Professor Alan Woodward, University of Surrey via Twitter @ProfWoodward

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 function. Once again, I am not submitting any suggested Confidential Annex to this report to the Prime Minister[3]. I do not consider that such an annex is presently necessary. That does not mean that one may not be needed in the future.

1.7 2014 was a significant year, not least because Parliament passed new powers relating to the areas that I oversee; my reports to the Prime Minister were increased in frequency from annually to half-yearly; and, various reviews of the legislation and oversight were commissioned. In addition a number of cases relating to the legislation that I oversee were taken to the IPT, which has made partial determinations on several of them. I touch on all of these matters in more detail throughout this report.

1.8 My office has continued to undertake our audits of public authorities' use of these intrusive powers against existing legislation and to make recommendations to improve compliance. Overall the inspections carried out by my office show that the staff within the public authorities have a desire to comply with the legislation and to achieve high standards in the work that they carry out. There is a strong culture of compliance and of self reporting when things go wrong.

1.9 I do find it frustrating however when it is reported that my office has given the public authorities a clean bill of health. In this reporting year my office made over 400 recommendations to public authorities to improve compliance or to improve the systems and procedures for the interception of communications or the acquisition of communications data. This doesn't to me translate in to a clean bill of health. My office continues to challenge positively the necessity and proportionality justifications put forward by the public authorities to ensure that the significant privacy implications are always at the forefront of their minds when they are working to protect the public in the interests of national security, to save life or to prevent or detect crime. There is however always room for improvement and the work that my office undertakes assists public authorities to keep their systems and their use of these intrusive powers under constant review.

1.10 Understandably, there is significant public debate at present not only about the privacy implications of the public authorities' use of these intrusive powers, but also about the capabilities that the public authorities might require, the adequacy of the existing legislation and, the effectiveness of the current oversight mechanisms. It is unhelpful and inaccurate when the debate is framed as privacy vs. security as though you can have one but not the other.

1.11 The key challenges for the future as I see them are to ensure that the United Kingdom (UK) has legislation governing interception and communications data techniques that provides reasonable clarity and forseeability, contains adequate human rights protections and provisions for the retention, storage, access to, sharing of and

3 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.

destruction of material and data and, which provide effective oversight mechanisms and rights for effective remedy. It is a considerable task, not least because of the global nature of the technologies that we are concerned with, but there have already been some positive steps forward.

1.12 There is a diverse range of interested and informed parties who can, are and should continue to contribute to the debates to ensure they are informed and accurate. Section 3 of this report sets out the considerable work my office has undertaken to engage in the debate and will demonstrate our commitment to understanding the key issues and to better informing the public about our work. There is, however, much more work to be done and my office will continue to contribute to the various debates and reviews by providing independent, accurate and unbiased advice and substantive evidence that is not affected by political persuasion.

1.13 Once again 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.

Section 2
My Role

2.1 I was appointed as Commissioner in January 2013. 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), although I do have limited duties under Part III of RIPA 2000. I also have non-statutory responsibility for overseeing the interception of communications in prisons in England, Wales and Northern Ireland. In addition I have recently been asked by the Prime Minister and have agreed to formally oversee directions under Section 94 of the Telecommunications Act 1984.


The Rt Hon. Sir Anthony May

RIPA Part I

2.2 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.

2.3 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 is limited to interception within the United Kingdom.

Interception of communications

2.4 **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[4]. 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).

2.5 The requirements of Chapter I of Part I RIPA 2000 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),

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

(5) and (9)). At the time of writing this report a revised draft code of practice is out for public consultation[5].

Communications Data

2.6 The structured procedure required by Chapter II of Part I RIPA 2000 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 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)).

2.7 The provisions of Chapter II of Part I RIPA 2000 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. A revised draft code of practice has recently been consulted on[6].

My main powers and duties

2.8 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 Chapter II of Part I, that is those relating to the acquisition and disclosure of communications data;
- the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties conferred or imposed on him by or under Part III; 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; and, so far as applicable to Part I material, those imposed by section 55.

2.9 In short, I am required to audit the interception of communications and the acquisition and disclosure of communications data under RIPA 2000 Part I, and any notices issued by the Secretary of State under Part III for the disclosure of protected information.

5 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf

6 https://www.gov.uk/government/publications/communications-data-draft-codes-of-practice-acquisition-disclosure-and-retention

2.10 I also have a responsibility to investigate unintentional electronic interception (not related to trying to put into effect an interception warrant) which attracts a civil penalty[7] under section 1(1A) of RIPA 2000. This complaints function came into force in 2011 as the European Commission identified deficiencies in the way in which the Data Protection Directive and the E-Privacy Directive were transposed.

2.11 I am not involved with matters under RIPA 2000 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

2.12 Section 6 of the Data Retention and Investigatory Powers Act (DRIPA) 2014 amends RIPA 2000 by requiring me to report on a half-yearly basis to the Prime Minister. The timing of the reports is as soon as is practicable after the end of each calendar year and after the end of the period of six months beginning with the end of the calendar year. As such the timing of my first report post DRIPA coincided with the timing that my next annual report would have been due anyhow.

2.13 I am required by section 58(2) to report to the Prime Minister contraventions of the provisions of RIPA 2000 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 IPT. I am not aware of any such report by the IPT which bears on my responsibilities. The Errors sections of this Report (see 6.82 - 6.97 & 7.96 - 7.109) constitute a principal part of the performance of the requirements of section 58(2).

2.14 Section 57(3) of RIPA 2000 provides that I shall give the IPT all such assistance (including my opinion as to any issue falling to be determined by the IPT) as the IPT may require in connection with its investigation of any matter; or otherwise for the purposes of its consideration or determination of any matter. In the last reporting year the IPT asked my office for assistance in connection with one matter under investigation and I can report that the IPT has already asked for assistance on a couple of matters under investigation in 2015.

Disclosure to the Commissioner

2.15 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

7 See http://iocco-uk.info/sections.asp?sectionID=2&chapter=6&type=top for more information

and communications data activities to which RIPA 2000 Part I relates however sensitive these may be.

Prisons

2.16 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 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.

Support to the Commissioner

2.17 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.

2.18 I am supported in my role by the Head of IOCCO Joanna Cavan, a team of nine IOCCO inspectors and two secretarial staff. The inspectors are independent, highly skilled and experienced in the principles and detail of RIPA Part I. The inspectors have been recruited from a wide variety of backgrounds, and bring with them a broad range of experience working with police forces, intelligence and law enforcement agencies, industry regulators, universities and telecommunications-related private organisations. Their experience covers analytical expertise, criminal and counter-terrorism investigations, forensic telecommunications, training and lecturing in both the technical and legislative aspects of communications data and covert investigations, and acting as accredited Single Points of Contact (SPoCs), Senior Responsible Officers (SROs) and Designated Persons (DPs).

2.19 My office has a strategic relationship with the Communication Service Providers (CSPs). This greatly assists us to carry out thorough inspections of the requirements made of them to disclose communications data and their ability to comply with warrants relating to the interception of communications. For example, on a regular basis the CSPs share with us their audit files which contain the name of the public authority acquiring data, the reference number of the request, the data description and the statutory purpose used. This information allows us to perform a back audit when inspecting public authorities to check that there is a corresponding authorisation in place and its scope.

2.20 On a number of occasions over the past two years we have sought the advice of, or commissioned, experts to assist us to carry out our independent inquiries and oversight. Our recent work on the journalist inquiry (see section 7) and some of last year's work in relation to the Snowden-related media revelations has demonstrated the value

of working with academics, technical experts and privacy advocates. My office intends to continue to engage with and seek advice from key individuals with expertise in relevant fields. I am also aware that my office would benefit from more resource and expertise in some key areas, such as technical and legal.

2.21 I was interested to learn that one of our international counterparts, the Dutch Review Committee on the Intelligence and Security Services (CTIVD), has a formal power to commission experts to perform certain tasks, for example to support the CTIVD to closely monitor, advise and inform it on the relevant technological, legal and societal developments, or to provide feedback on the contents, coherence and relevance of investigations and reports. This is a good initiative.

Section 3
Transparency and Accountability

3.1 My half-yearly reports, my office's appearances before the various parliamentary select committees, our additional reports, other publications and public engagements seek to provide the public and Parliament with greater understanding, evidence and assurance of my role and the way in which interception and communications data powers are being used by public authorities and the safeguards in place. My last report had, for the first time, no confidential annex and sought to bring a rigorous and independent assessment of the matters my office oversees, especially given the public concern in the aftermath of the Snowden-related media reports.

3.2 I do not presently regard that simply reporting annually, or indeed half-yearly, provides the public with sufficient information about the work we are engaged in. Understandably, there is significant public concern at present about the privacy implications of public authorities' use of these intrusive powers, the capabilities that the public authorities might require, the adequacy of the existing legislation and, the effectiveness of the oversight. This may change in future but in the meantime it is important for my office to continue to engage publicly, in so far as it is possible to in addition to carrying out our statutory function, to help inform the various debates and reviews.

3.3 The comments in our last two annual reports and our recent written submission to the Investigatory Powers Review[8] set out the need for enhanced and accurate statistical requirements to bring clarification as to the volumes and types of communications data acquired by public authorities. We are pleased that the Home Office has taken on board our recommendations in this respect and have included enhanced statistical requirements in the revised code of practice[9] accompanying Chapter II of Part I RIPA 2000. These new requirements will go some way to improving transparency. That said, the new statistical requirements will need to be explained in a way that makes them easy to interpret and meaningful so as to contribute towards improved accountability.

3.4 Since the publication of my last report my office has been delighted to accept invitations to speak publicly about our role at numerous events including;

- the International Communications Data and Digital Forensics Conference;
- the Internet Service Providers Association (ISPA) event hosted by Bird & Bird;
- the National Anti-Fraud Network (NAFN) Annual Summit;
- the Wilton Park 'Privacy, security and intelligence in the digital age' conference;
- Matrix Chambers' event about the legality of state surveillance post-Snowden;
- the Oxford Intelligence Group's - Snowden, the media and the state event;
- the Computers, Privacy and Data Protection Conference, and,
- the Scottish Public Law Group Surveillance event.

8 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

9 https://www.gov.uk/government/publications/communications-data-draft-codes-of-practice-acquisition-disclosure-and-retention

3.5 My office has also attended and / or taken part in various events, roundtables and panel discussions including: the International Intelligence Review Agencies Conference (IIRAC); a Workshop on the Data Retention and Investigatory Powers Act 2014; the Parliament and Internet Conference; the Bingham School of Law Investigatory Powers Review event; and the National Union of Journalists (NUJ) and Guardian event 'Journalism in the age of mass surveillance: Safeguarding journalists and their sources'. At the IIRAC conference we had the opportunity to meet a number of our international counterparts and we have since hosted a number of them to discuss in further detail our respective oversight regimes.

3.6 My office has engaged with various think tanks and civil society organisations to discuss key issues and concerns. Throughout the year we have also given evidence to various committees including the Home Affairs Select Committee (HASC) and the Intelligence and Security Committee (ISC).

3.7 Throughout the year we have published various documents on our website (www.iocco-uk.info) providing further information about the work we are undertaking. We have issued press statements regarding matters under investigation and published the findings of inquiries we have undertaken. In July 2014 we created our Twitter account @iocco_oversight. This has improved our communication, helped us to distribute news, engage with and answer questions from the public and given us access to a wealth of opinion and debate about our work. It helps us to keep up to date with relevant news and is also a valuable tool for following discussions and gleaning new information from academics, researchers, lawyers, civil society, think tanks, computer scientists, network engineers and other key individuals working in relevant fields.

3.8 I hope that this work has demonstrated our commitment to understanding the key issues and provided the public with more information about our oversight.

3.9 In my view there is more the intelligence agencies, police forces and law enforcement could do, and should do, to better inform the public about how they use their powers under RIPA 2000, why they need these intrusive powers and, why additional powers might be required.

Section 4
Reviews of RIPA Legislation and Oversight

4.1 A number of reviews were commissioned during 2013/14 and several strands of the reviews are relevant to the legislation that I oversee or to the oversight mechanisms more generally.

4.2 The reviews have much to consider and they are yet to report. We do, and will continue to, engage with all of the reviews to share our experiences, concerns, observations and findings and provide any other information which may assist. If there need to be changes to the way we operate or are organised we look forward to future consultations to consider such issues and how they can be developed and implemented. A summary of each review and the assistance we have provided is below:

1 **Privacy and Security Inquiry[10] by the Intelligence and Security Committee (ISC)**

Commissioned on 17th October 2013, the inquiry seeks to examine the laws which govern the intelligence agencies' ability to intercept private communications. In addition to considering whether the current statutory framework governing access to private communications remains adequate, the ISC will also be considering the appropriate balance between our individual right to privacy and our collective right to security.

The Rt Hon. Sir Paul Kennedy (interim Interception of Communications Commissioner) and Joanna Cavan (Head of IOCCO) gave oral evidence to the ISC in relation to this inquiry on 30th October 2014. This was a private session at the request of the ISC.

2 **Independent Surveillance Review[11] by the Royal United Services Institute (RUSI)**

This review, announced by the Deputy Prime Minister on 4th March 2014, will:

- advise on the legality, effectiveness and privacy implications of the UK surveillance programmes, particularly as revealed by the 'Edward Snowden case';
- examine potential reforms to current surveillance practices, including additional protections against the misuse of personal data, and alternatives to the collection and retention of bulk data; and,
- make an assessment of how law enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity, and privacy.

Joanna Cavan (Head of IOCCO) attended a roundtable with the Independent Surveillance Review panel on Tuesday 24th February 2015 to discuss the role of the independent Commissioners in the oversight and accountability of public authorities.

10 http://isc.independent.gov.uk/public-evidence

11 https://www.rusi.org/news/ref:N53D2226896081/

3 Investigatory Powers Review [12]

This is a statutory review with all-party agreement under section 7 of the Data Retention and Investigatory Powers Act (DRIPA) 2014 on the capabilities and powers required by law enforcement and the security and intelligence agencies and the regulatory framework within which those capabilities and powers should be exercised. David Anderson QC, the UK's Independent Reviewer of Counter Terrorism Legislation, is leading the first part of the review which is due to report before the election.

My office submitted written evidence to this review which commented on:

- the effectiveness of the current statutory oversight arrangements;
- the safeguards to protect privacy;
- the case for amending or replacing legislation; and
- the statistical and transparency requirements that should apply.

We published our written evidence in full to this review via our website on 5th December 2014[13].

12 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330749/Review_of_Communications_Data_and_Interception_Powers_Terms_of_Reference.pdf

13 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

Section 5

The Data Retention and Investigatory Powers Act (DRIPA)

5.1 DRIPA[14] received Royal Assent on 17th July 2014. My office published its full response[15] shortly thereafter. To meet the requirements expressed by Parliament during the passing of the Bill, my office committed to, in my next report, in addition to reporting on the general carrying out of my functions, report on whether DRIPA 2014, in practice, does exactly what the Government said it would –

> *".....reassure people that the Bill does exactly what the Government are saying: it merely replaces the powers already in existence ..... The commissioner currently reports annually on these matters, and the Opposition proposal, as I understand it, is that he would report on a six-monthly basis. He would, therefore, not just be looking at the situation, but reporting on what was happening. Were he [the Interception Commissioner] to find that there was an extension of powers that would be made clear to the people....."*
>
> *Home Secretary – Hansard – Column 708*

5.2 The Shadow Home Secretary made similar reference -

> *"The six monthly review will reassure the House that the Bill is being implemented in the way that Parliament intended"*
>
> *Yvette Cooper MP – Hansard – Column 724*

5.3 In this section of the report I will therefore try to answer the question as to whether DRIPA is doing what was intended. To answer this question my office has focused its consideration on the operational effect of sections 3, 4 and 5 of DRIPA 2014 and whether there have been any changes in practice or consequences not anticipated. My office has not been able to consider the operational effect of section 1 of DRIPA 2014 for reasons which I will also outline. In addition I will discuss our new reporting requirements under section 6 of DRIPA 2014.

Section 1 DRIPA. Requirements for CSPs to retain communications data

5.4 Our full response to DRIPA 2014 noted that there does not appear to be a legal requirement for the Interception of Communications Commissioner or any other independent oversight body to review either a) the implementation of section 1 DRIPA 2014. This gives the Secretary of State the power to give a retention notice to a public telecommunications operator requiring it, the operator, to retain relevant communications data; or, b) whether DRIPA 2014 makes provision for the imposition of wider retention requirements than could be imposed under the Data Retention (EC Directive) Regulations 2009 which section 1 of DRIPA 2014 sought to replace. While the

14 https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014

15 http://www.iocco-uk.info/docs/IOCCO%20response%20to%20new%20reporting%20requirements.pdf

Information Commissioner[16] has a role in respect of data retained in compliance with a retention notice, that role is to ensure compliance with the data protection principles[17] (for example, data security, the lawful processing of the data and business processes to stop over retention).

5.5 My office is therefore not in a position to clarify or report on matters relating to the giving of a retention notice by a Secretary of State under DRIPA 2014.

Section 3 DRIPA. Statutory purpose of economic well-being in RIPA Part I.

5.6 As a consequence of the Privacy and Electronic Communications Directive 2002/58 ("the E-Privacy Directive")[18] matters relating to the interception of communications or the acquisition of communications data, where they relate to the economic interests of the United Kingdom, should directly relate to "state security".

5.7 The E-Privacy Directive came into effect two years after RIPA 2000 came into force and so the code of practice for the interception of communications and the code of practice for the acquisition and disclosure of communications (made under section 71 of RIPA 2000) explained where the interception of communications or the acquisition of communications data is necessary in the economic interests of the United Kingdom, it must be taken into account whether, on the facts specific to the case, it is directly related to state security.

5.8 The term "state security," which is used in the E-Privacy Directive should be interpreted in the same way as the term "national security" which is used in RIPA 2000 and the accompanying codes of practice to Part I.

5.9 Section 3 of DRIPA therefore clarifies in primary legislation, by amending sections 5(3)(c) and 22(2)(c) RIPA 2000, the requirement imposed by the E-Privacy Directive and already set out in the codes of practice that interception warrants can only be issued and communications data can only be acquired on the grounds of economic well-being when specifically related to national security. The relevant provisions of RIPA 2000 are amended to read as follows:

> section 5(3)(c) *"For the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the United Kingdom"*
>
> section 22(2)(c) *"in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security."*

16 http://ico.org.uk/

17 http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles

18 The E-Privacy Directive" sets out the requirements for the processing of personal data and protection of privacy in the electronic communications sector

5.10 The policy effect has been to take account of the E-Privacy Directive; I can confirm that it has not changed or amended the extent to which the powers have been used.

Section 4 DRIPA. Extra-territorial reach of RIPA Part I.

5.11 Part I RIPA 2000 has always had implicit extraterritorial effect. Some companies based outside the United Kingdom (UK), including some of the largest communications providers in the market, questioned whether the legislation applied to them. These companies argued that they would only comply with requests where there was a clear obligation in law, albeit the majority have always assisted in exigent circumstances where they are satisfied there is an emergency that involves death or serious harm.

5.12 When RIPA Part I was drafted, some 15 years ago, it took account of the changes in mobile and Internet based telecommunication systems, in particular, the realisation that not all of the system parts were within UK territory, that devices and services could operate both within and outside of the UK and that services do not necessarily relate to a company based within the UK. Part I was intended to apply to telecommunications companies offering services to UK users, wherever those companies and / or their telecommunication systems were based.

5.13 When RIPA came into force in 2000 it recognised that devices could be used in and move between different geographic locations and that a user of a communications service could be within the UK but the telecommunications system on which the service relied could be largely outside the UK (for example internet-related electronic mail or 'webmail'). The following are examples of how RIPA 2000, before amendment by DRIPA 2014, made provision for such circumstances:

- section 21(6)(a) explains traffic data includes any data identifying or purporting to identify, any person, apparatus or location to or from which, or by means of which the communications is or may be transmitted;
- section 2(1) explains a 'telecommunication system' means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

5.14 Section 4 of DRIPA 2014 amends RIPA 2000 to put beyond doubt the extra-territorial reach in relation to both the interception of communications and the acquisition of communications data by inserting new subsections into sections 11 (implementation of interception warrants) and 12 (maintenance of interception capability), which are concerned with interception and, section 22 which is concerned with the acquisition of communications data. This confirms that overseas companies that are providing communications services within the UK are subject to UK legislation with respect to lawful requests for interception and communications data.

5.15 Section 4(4) DRIPA 2014 amends section 11 of RIPA 2000 (implementation of interception warrants) by inserting a new subsection (5A), which sets out factors to be taken into account whether steps for giving effect to a warrant are reasonably practicable. That amendment takes account of restrictions that laws in the countries or territories outside the UK might impose on the persons upon whom a requirement might be levied.

5.16 Section 4(8) DRIPA 2014, which amends section 22 of RIPA 2000 (obtaining and disclosing communications data), does not appear to take account of any laws in the country or territory outside of the UK and any restrictions that might be in place that could prohibit the disclosure sought.

5.17 The larger element of our inspection regime is to engage with all police forces, law enforcement agencies, the intelligence agencies and other public authorities who may undertake the acquisition of communications data in accordance with Chapter II of Part I of RIPA 2000. During these inspections my office has asked the question as to whether Accredited Officers (AOs) within the Single Points of Contact (SPoCs) have been aware of the changes to RIPA brought about by DRIPA, in particular, the extra-territorial effect of notices served on overseas CSPs. Several examples have been shared with us by those using their powers to acquire communications data from CSPs outside of our territory albeit the SPoCs were, in practice, mostly unaware of the amended extra-territorial effect of the notice.

5.18 Their general observations are that whilst the overseas CSPs take receipt of notices requiring the disclosure of data, the CSPs continue to maintain that the notices cannot be enforced or compelled through civil sanction within the UK as the CSP is outside of UK jurisdiction. It is common for the CSPs to require information in addition to the notice to determine whether they are able to disclose communications data taking into account the laws within the jurisdiction in which they generate and retain the data. In the CSPs view they are disclosing the data "voluntarily" and are not required to disclose it.

5.19 For example, one SPoC recently shared with our inspectors that an overseas CSP had declined a notice requiring the disclosure of internet-related data as they required additional information about the nature of the investigation to enable them to consider the laws they are subject to and determine whether they were able to "voluntarily" disclose the data. In practice this is common as the additional information assists the overseas CSP to determine if the criminal act within the UK infringes their user agreements and / or laws within their jurisdiction.

5.20 Turning to interception warrants, some overseas CSPs are providing assistance in very limited circumstances.

5.21 The policy effect of the amendments has been to make explicit that which was implicit in RIPA concerning extra-territorial reach. I can report however that this does not appear to have changed or amended the operational practice of those public authorities using their powers under Part I, or the conduct undertaken by overseas CSPs. Furthermore there remain a number of CSPs who still do not recognise or consider that they are bound by RIPA 2000.

Section 5 DRIPA. The definition of "telecommunications service".

5.22 The original definition within section 2(1) of RIPA stated that -

> *"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).*

5.23 Section 5 of DRIPA 2014 inserted a new subsection into section 2 of RIPA, (8A), to make clear that the definition of "telecommunications service" includes companies that provide internet-based services, such as webmail. The following text is now included after section 2(8) RIPA 2000 -

> *"(8A) For the purposes of the definition of "telecommunications service" in subsection (1), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system."*

5.24 One of the consequences of the change to the definition is that it clarifies the telecommunication services that are covered by Part I of RIPA so that it is more difficult for companies who provide internet-based services, such as webmail, to argue that they are not caught by RIPA 2000.

5.25 I can report that the change to the definition does not appear in practice to have resulted in an extension of powers.

Section 6 DRIPA. Requirements for half-yearly reports by the Interception of Communications Commissioner

5.26 Section 6 of DRIPA 2014 amends RIPA 2000 by requiring half-yearly reports by the Interception of Communications Commissioner. The timing of the reports is as soon as is practicable after the end of each calendar year and after the end of the period of six months beginning with the end of the calendar year. As such the timing of my first report post DRIPA coincided with the timing that my next annual report would have been due anyhow.

5.27 It is important to set out that our intention is to continue to report the statistical information relating to the use of the powers and the findings from our inspections on an *annual* basis (in the first report of each year). This is because the statistical information takes two months to collate and analyse and it would be futile to complete that exercise twice-yearly and, our inspections of the larger volume users of communications data powers occur on an annual basis so reporting the findings and recommendations of these inspections twice-yearly would provide an incomplete picture which could serve to mislead. Section 3 of this report has already described that my office has been publishing

information about the work we have been undertaking on a more regular basis for some time. Furthermore, section 58(5) of RIPA 2000 has always had provision for the Interception of Communications Commissioner to also make *"any such other report to the Prime Minister on any matter relating to the carrying out of the Commissioner's functions as the Commissioner sees fit."* I used this provision recently to publish the findings from my office's inquiry into the acquisition of communications data to identify journalistic sources. This enables us to report promptly with a higher degree of flexibility than the half-yearly reports which must be laid before each House of Parliament and therefore we intend to continue in this vein regardless of the new reporting requirement.

Section 6
Interception of Communications

6.1 In this section I shall provide an outline of the interception legislation, give details of the interception inspection regime, provide statistical information about the use of interception powers and outline the key findings from my office's inspections.

6.2 Prior to doing that, I think it worth pointing out that my office is constrained by the statutory secrecy provisions in section 19 of RIPA 2000 forbidding disclosure of certain aspects of interception, for example, the existence and contents of a warrant and of any section 8(4) certificate in relation to a warrant; the steps taken in pursuance of a warrant; everything in the intercepted material, together with any related communications data etc. This does make transparency challenging in this area of our work.

6.3 For those who want to know more about the technical infrastructure requirements, operational requirements, and hand-over interfaces relating to interception a significant amount of information is published by the European Telecommunications Standards Institute[19].

Applications for Interception Warrants

6.4 Part I of RIPA 2000 provides that the interception of communications can be authorised with a warrant issued by the Secretary of State under section 5(1). The conduct authorised by an interception warrant includes any conduct necessary to obtain the content of the communication and any related communications data (as defined in section 20 and Chapter II of Part I RIPA 2000).

6.5 **Applicant.** An interception warrant cannot be issued except in response to an application made by or on behalf of the persons listed in section 6(2) of RIPA 2000, who are:

- the Director General of the Security Service (MI5);
- the Chief of the Secret Intelligence Service (SIS);
- the Director of the Government Communications Headquarters (GCHQ);
- the Director General of the National Crime Agency (NCA);
- the Commissioner of the Metropolitan Police;
- the Chief Constable of the Police Service of Northern Ireland (PSNI);
- the Chief Constable of the Police Service of Scotland;
- the Commissioners of Her Majesty's Revenue and Customs (HMRC);
- the Chief of Defence Intelligence.

6.6 **Secretaries of State.** Interception warrants have to be authorised personally by a Secretary of State (sections 5(1) and 7(1)(a)). He or she has to sign the warrant personally, or in an urgent case to authorise the issue of a warrant signed by a Senior Official (section

19 See http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception and also http://www.europarl.europa.eu/hearings/20000222/libe/framework/eplegs/default_en.htm#UK

7(1)(b)).

6.7 In practice four Secretaries of State and one Scottish Minister consider most of the interception warrants. They are:

- the Defence Secretary;
- the Foreign Secretary;
- the Home Secretary;
- the Secretary of State for Northern Ireland; and
- the Cabinet Secretary for Justice for Scotland[20].

6.8 Each Secretary of State has Senior Officials and staff in their warrant granting department (WGD) whose functions include scrutinising warrant applications for their form, content and sufficiency, and presenting them to the Secretary of State with appropriate suggestions.

6.9 **Statutory necessity purposes**. The Secretary of State may not issue 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[21];
- for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security[22], of safeguarding the economic well-being of the United Kingdom; or
- for the purpose in circumstances equivalent to those in which the Secretary of State would issue a serious crime warrant of implementing an international mutual assistance agreement (section 5(3)).

6.10 These statutory purposes and the requirement of necessity come directly from Article 8 of the European Convention on Human Rights (ECHR). To issue an interception warrant for any other purpose would be unlawful. It is part of my function to make sure that all warrants are issued for these statutory purposes only.

6.11 **Proportionality.** The Secretary of State may not issue 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.

---

20 Interception warrants to prevent or detect serious crime may be authorised by Scottish Ministers, 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.

21 Section 81(3) of RIPA 2000 defines "serious crime" as a crime for which an adult first-time offender could reasonably expect a sentence of three years' custody or more, or which involves the use of violence, substantial financial gain or conduct by a large number of persons in pursuit of a common purpose.

22 As amended by Section 3 of the Data Retention and Investigatory Powers Act (DRIPA) 2014.

6.12 Proportionality pervades human rights jurisprudence and is a thread which runs through RIPA 2000. Every application for an interception warrant must address it explicitly. Secretaries of State have to address proportionality when deciding whether to issue an interception warrant. In doing so they have to balance (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 sought could reasonably be obtained by 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.

Interception Warrants

6.13 All interception warrants are for the interception of communications (access to content) and the acquisition of related communications data. Section 5(6)(a) says that the conduct authorised by an interception warrant shall be taken to include 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.

6.14 Applications for interception warrants should contain the information included in Paragraph 4.2 or 5.2 of the code of practice. They contain detailed explanations and supporting information including specific sections about the protection of privacy, to help the Secretary of State assess the merits of the application.

6.15 Interception warrants have an initial duration of 6 months where the statutory purpose is national security or economic well-being 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.

6.16 The Secretary of State may personally renew an interception warrant before the end of its validity period but only if he or she 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 must justify the necessity for renewal, giving an assessment of the intelligence value of the interception to date. Renewal takes effect from the date on which the Secretary of State signs the renewal instrument.

6.17 The Secretary of State is required to cancel an interception warrant if 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 agencies should keep their warrants under continuous review and apply to cancel any warrant that is no longer necessary. In practice, cancellation instruments will be signed by a Senior Official on behalf of the Secretary of State (paragraph 4.16 of the code of practice).

6.18 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 working days unless it is renewed by the Secretary of State (section 9(6)(a)).

6.19 Interception warrants may be issued subject to the provisions of either section 8(1) or section 8(4) of RIPA 2000.

6.20 **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 and any association or combination of persons.

6.21 An application for 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 person or premises constituting the subject of the application;
- a description of the communications to be intercepted;
- an explanation of why the interception is necessary under section 5(3);
- an explanation of why the conduct is proportionate;
- consideration of any unusual degree of collateral intrusion, not least if the communications might be privileged or confidential; and
- an assurance that all intercepted material will be handled in accordance with the safeguards required by section 15 of RIPA 2000.

6.22 Section 8(1) warrants have to comprise one or more schedules with details designed to tell the relevant CSPs or other persons providing assistance what communications they are required to intercept (section 8(2)).

6.23 **Section 8(4) interception warrants.** Section 8(4) warrants are only for the interception of external communications, namely those sent or received outside of the British Islands (section 20). A section 8(4) warrant does not have to name or describe a person as the interception subject or a single set of premises as the target of the interception.

6.24 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; and
- 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)) as mentioned in sections 5(3)(a), (b), or (c).

6.25 By virtue of section 8(5)(b) an interception warrant may also authorise other conduct as described in section 5(6). Such conduct includes the interception of communications

not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises.

6.26 An application for a section 8(4) warrant should contain the details required by paragraph 5.2 of the code of practice. The required details include:

- the background of the operation;
- a description of the communications to be intercepted;
- a description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate;
- the certificate that will regulate examination of intercepted material;
- an explanation of why the interception is necessary under section 5(3);
- an explanation of why the conduct is proportionate;
- a consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances, not least if the communications might be privileged or confidential;
- an assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2) to 16(6) of RIPA 2000; and
- an assurance that all intercepted material will be handled in accordance with the safeguards required by section 15 and 16 of RIPA 2000.

6.27 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 Chapter I of Part I RIPA 2000 statutory purpose. Examination of material for any other purpose would be unlawful.

6.28 **Safeguards.** These apply to all interception warrants. Section 15(2) strictly controls the disclosure and/or copying of intercepted material, requiring it to be limited to the minimum necessary for the authorised purposes. All intercepted material must be handled in accordance with safeguards which the Secretary of State has approved under RIPA 2000. Section 15(3) requires that every copy of intercepted material and any related communications data are destroyed as soon as there are no longer grounds for retaining it for any of the authorised purposes.

6.29 **Additional safeguards for section 8(4) interception warrants.** There are extra safeguards in section 16 for section 8(4) warrants and certificates. The section 8(4) intercepted material may only be examined to the extent that its examination:

- has been certified as necessary for a Chapter I of Part 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.

6.30 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).

6.31 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 that its examination is necessary for a statutory purpose in relation to a specific period of not more than 6 months for national security or 3 months for serious crime or economic well-being. Since this certification has to relate to an individual, it is broadly equivalent to a section 8(1) warrant.

6.32 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) certification for that person to be duly applied for without losing what could be essential intelligence.

6.33 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 made on the basis of factors 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 authority issued in accordance with section 16(3) or 16(5);
- the section 8(4) structure does not permit random trawling of communications. This would be unlawful. It only permits a search for communications the examination of which has been certified as necessary for a statutory purpose.

6.34 **Selection of section 8(4) material.** In my 2013 Annual Report I outlined that my clear independent judgement was that the interception agencies were not operating the selection procedures unlawfully or to the outer limits of legality, so as to produce disproportionate invasion or potential invasion of people's privacy subject to three caveats. I made the point that only the third caveat should be seen (subject to my further inquiry) as suggesting the possibility of some structural or other reconsideration.

6.35 The three caveats were 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 of my 2013 Annual Report) 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. I provide an update on this work in paragraphs 6.60 to 6.65 of this report.

2 the Errors Section of my 2013 report (and the comparative section in 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.

3 I needed to undertake further detailed investigation into the actual application of individual selection criteria from stored selected material initially derived from section 8(4) interception.

6.36 I will come back to (3) but first it is pertinent to note that since my 2013 report and subsequent investigations there have been several cases taken to the IPT which are relevant to my area of oversight. The case of Liberty & Others vs. the Security Service, SIS and GCHQ[23], is particularly relevant to the operation of the section 8(4) process. In the Judgment dated 5th December 2014 the IPT made a declaration that the regime in respect of interception under sections 8(4), 15 and 16 of RIPA 2000 does not contravene Articles 8 or 10 of the European Convention on Human Rights (ECHR) and does not give rise to unlawful discrimination contrary to Article 14, read together with Articles 8 and/or 10 of the ECHR. A further Judgment dated 6th February 2015 declared that prior to the disclosures made by the respondent, the regime governing intelligence-sharing contravened Articles 8 or 10 ECHR[24]. There are still outstanding matters regarding the proportionality and lawfulness of any alleged interception of the Claimants' communications to be determined. Furthermore at the time of drafting this report, a revised draft of the interception of communications code of practice is out for public consultation[25] and section 7 includes additional information on the safeguards that exist for the interception and handling of external communications under section 8(4) of RIPA 2000, including how the section 16 procedures are applied.

6.37 In 2014 my office carried out the further investigations into the actual application of individual selection criteria as mentioned at (3) above and, in particular reviewed the breadth and depth of the internal procedures for the selection of material to ensure that they were sufficiently strong in all respects. These investigations, which focused on GCHQ as the interception agency that makes the most use of section 8(4) warrants and selection criteria, addressed in good detail the selection criteria and related matters.

6.38 In brief, prior to analysts being able to read, look at or listen to material, they must first provide a justification which includes why access to the material is required, consistent with, and pursuant to, section 16 and the applicable certificate (i.e. how the requirement is linked to one of the statutory necessity purposes and is a valid intelligence

23 See IPT/13/77/H http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf

24 http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

25 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf

requirement), and why such access is proportionate. Although I consider that the selection procedure is carefully and conscientiously undertaken both in general and, so far as we were able to judge, by the individuals concerned, this process relies mainly on the professional judgement of analysts, their training and management oversight. There is no pre-authorisation or authentication process to select material.

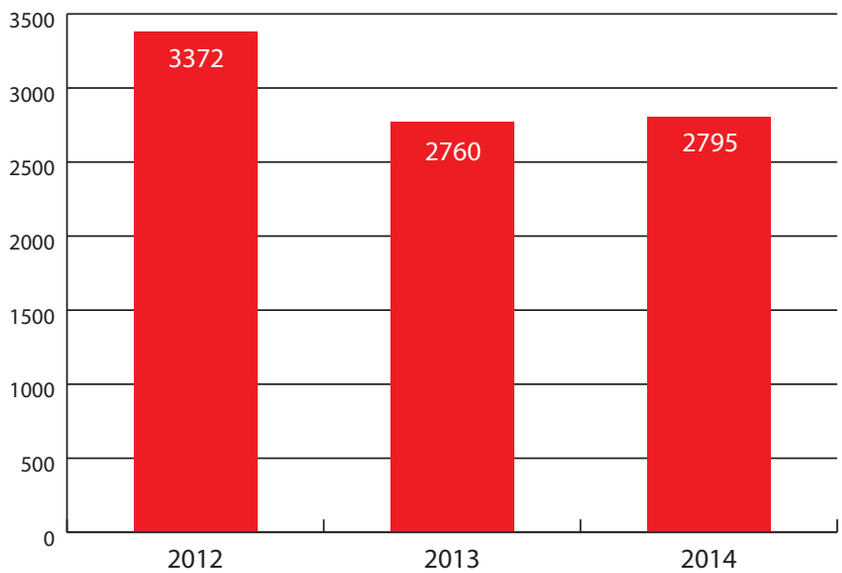
6.39 However, random audit checks are conducted retrospectively of the justifications for selection, by or under the direction of GCHQ's Internal Compliance Team, and, in addition, the IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use. The results of the retrospective audits are provided to my office during our inspections and any breaches of the section 15/16 safeguards will have already been reported to my office (see errors section of this chapter). Although the retrospective audits are a strong safeguard and also serve to act as a deterrent against malign use, I consider that a number of matters need further thought including whether it might be feasible (or indeed desirable) to introduce some sort of pre-authorisation or authentication process, or whether the retrospective audits could be broadened and enhanced. If the retrospective audits were enhanced and did not indicate any systemic compliance issues, then that would seem to provide sufficient evidence that the safeguards are adequate and are being appropriately applied. GCHQ has undertaken a significant amount of work to consider and scope these matters with both the technical and analytical communities to assess their feasibility and to evaluate the impact on the business. These changes would be significant. Another option might be for my office to have a more explicit role in this audit process in the same way as we do when reverse auditing communications data requests disclosed by CSPs and auditing the streamlining procedures under Chapter II of Part I of RIPA 2000 (see Section 7 of this report for more detail). At present the Commissioner is only responsible under section 57(1)(d) for reviewing the adequacy of the arrangements as a whole under section 15 (and 16).

6.40 The related matters that my office investigated included the detail of a number of other security and administrative safeguards in place within GCHQ (which are not just relevant to interception work). These included the security policy framework (including staff vetting), the continuing instruction and training of all relevantly engaged staff in the legal and other requirements of the proper operation of RIPA 2000 with particular emphasis on Human Rights Act requirements, and the development and operation of computerised systems for checking and searching for potentially non-compliant use of GCHQ's systems and premises. I was impressed with the quality, clarity and extent of the training and instruction material and the fact that all staff are required to undertake and pass a periodic online test to demonstrate their continuing understanding of the legal and other requirements.

Statistics for Interception Warrants

6.41 Figure 1 shows the number of new interception warrants issued in each of the years 2012-2014 for the nine interception agencies. The total number of warrants issued during 2014 was 2795, an increase of 1.3% on 2013.

Figure 1 *Total Number of Interception Warrants Issued 2012-14*



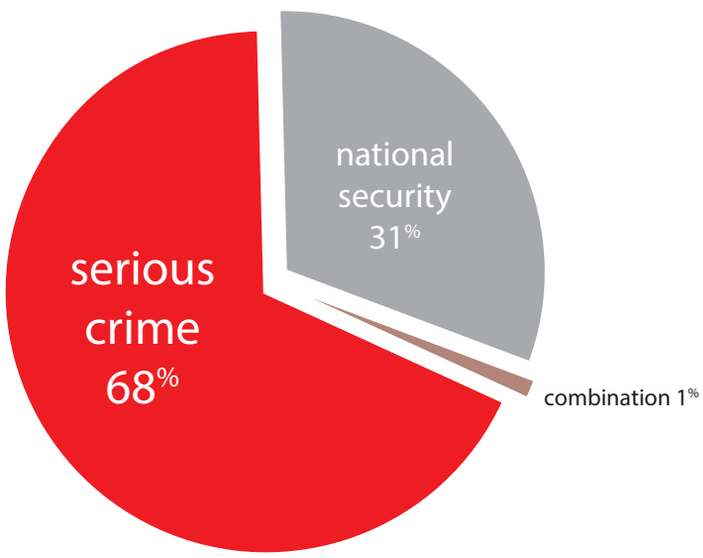
6.42 The total number of extant warrants on 31st December 2014 was 1605, a 3.8% decrease on 2013. Of the 1605 warrants, 20 were issued under section 8(4).

6.43 Some of the 1605 warrants were first authorised before 2014 but the vast majority of interception warrants do not run for longer than 6 months. Last year I commented that it was unsatisfactory that a number of the interception agencies have to apply to renew their warrants excessively early. This results in significantly shortened periods of authorisation. Serious crime warrants can only be authorised for a three month period and this means that an applicant may have to submit renewal paperwork only a few weeks after the initial interception was initially authorised. Understandably in some cases there has not been sufficient time to gain a detailed intelligence picture and as a result it can be hard to articulate the benefit and justify continuance. In addition renewing early causes the intervening authorisation period to be lost and therefore serious crime warrants of this kind are virtually never in force for the full three month period. A further consequence of early renewal is that warrants are often subject to unnecessary renewals. The majority of serious crime interception warrants do not last more than 6 months and therefore a renewal would not be necessary if the period was amended to 6 months. There remains a strong practical case for increasing the validity period for serious crime warrants to six months, or at least in amending the legislation to enable the renewal to take effect from the expiry of the original authorisation as this latter approach would not shorten the original authorisation period.

6.44 This year we provide a breakdown of the 2795 interception warrants issued by statutory necessity purpose to better inform the public as to how these intrusive powers are being used. Figure 2 details this further breakdown.

6.45 The combination category in Figure 2 represents those few warrants that were

Figure 2 *Warrants Issued by Statutory Purpose*



authorised for more than one statutory purpose. The vast majority of the serious crime warrants fell into one of the following five categories: unlawful supply of controlled drugs; firearms and violence; robbery and theft; financial crime; or smuggling / trafficking.

Inspection Regime

6.46 Objectives of Inspections. My office's interception inspections are structured to scrutinise the key areas covered by Chapter I of Part I RIPA 2000 and the associated code of practice. A typical inspection of an interception agency will include the following:

- a review of the action points or recommendations from the previous inspection and their implementation;
- an evaluation of the systems in place for the interception of communications to ensure they are sufficient for the purposes of Part I Chapter I of RIPA 2000 and that all relevant records have been kept;
- examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;
- interviews with case officers, analysts and/or linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
- examination of any urgent oral approvals to check the process was justified and used appropriately;
- a review of those cases where communications subject to legal privilege or

otherwise confidential information (e.g. confidential journalistic, or confidential medical) have been intercepted and retained, and any cases where a lawyer is the subject of an investigation;

- an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data;
- a review of the errors reported, including checking that the measures put in place to prevent recurrence are sufficient.

6.47 After each inspection my office compiles a detailed inspection report and action plan stating the findings and recommendations. This is sent to the head of the interception agency and is copied to the relevant Secretary of State and Warrant Granting Department (WGD).

6.48 My office's inspections of the four main WGDs have a slightly different emphasis. The WGDs undertake an important function which is comparable to the guardian and gatekeeper role performed by the Single Point of Contact (SPoC) for communications data applications under Chapter II of Part I of RIPA 2000. WGDs are a source of independent advice to the Senior Official and Secretary of State and perform a valuable pre-authorisation scrutiny of warrant applications and renewals to ensure that they are (and remain) necessary and proportionate. The emphasis during the WGD inspections is on the integrity of the authorisation process and the level of challenge applied to the warrants by the Secretaries of State and their Senior Officials. Last year my office introduced inspection reports and action plans for the WGDs which are also shared with the relevant Secretary of State.

6.49 **Inspection Reports.** My office's reports contain formal recommendations with a requirement for the interception agency or WGD to inform my office within two months on what progress has been made. The inspection reports contain operational detail which, under the terms of section 19(4) of RIPA, I may not disclose in detail. However, in general terms the reports include:

- an assessment of how far the recommendations from the previous inspection have been achieved;
- a summary of the number and type of interception documents selected for examination, including a detailed list of those warrants;
- detailed comments on all warrants selected for further scrutiny and discussion during the inspection;
- an assessment of the errors reported to my office during the inspection period;
- an account of the examination of the retention, storage and destruction procedures;
- an account of other policy or operational issues which the agency or WGD raised with my office during the inspection;
- a number of recommendations aimed at improving compliance and performance generally;

- an overall assessment of the interception agency's or WGD's level of compliance with RIPA.

6.50 I will describe some of the most frequent recommendations and a number of other matters arising from these inspections later in this section of the report.

6.51 **Number of inspections.** My office has maintained the pattern of inspecting all nine interception agencies and the four main WGDs twice yearly, making a total of 26 inspections. The length of each inspection depends on the volume of interception warrants and the complexity of the particular interception agency's operations. The inspections of the larger or more complex interception agencies are conducted by an inspection team of 2 or 3 and take place over 3 days twice-yearly. The inspections of the smaller volume users are generally conducted by an inspection team of 2 and generally last 1 or 2 days twice-yearly. As a point of principle we inspect each WGD after the interception agencies for which it is responsible. This provides an opportunity for my office to discuss the findings and recommendations from the interception agencies' inspections with the WGD. In addition to the twice-yearly inspections there are a number of additional visits and a large amount of correspondence throughout the year to follow up and review progress against recommendations, discuss other issues or matters arising, or to conduct investigations into errors.

6.52 **Examination of warrants.** My office inspects the systems in place for applying for and authorising interception warrants. This usually involves a three-stage process:

- First, to achieve a representative sample of warrants we select from across different crime types and national security threats. In addition we focus on those of particular interest or sensitivity, for example those which give rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period (in order to assess the continued necessity for interception), those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called 'thematic' warrants. More detail on some of these areas will be provided in the recommendations section of this report.
- Second, we scrutinise the selected warrants and associated documentation in detail during reading days which precede the inspections.
- Third, we identify those warrants, operations or areas of the process where we require further information or clarification and arrange to interview relevant operational, legal or technical staff, and where necessary we require and examine further documentation or systems in relation to those matters during the inspections.

6.53 **Samples.** The total number of warrants specifically examined during the 26 interception inspections was 936. This figure equates to 58% of the number of extant warrants at the end of the year and 34% of the total of new warrants issued in 2014. This figure is considerably higher than the number examined last year and this is due in part to the fact that we introduced a significant number of changes to the inspection procedures

in the second series of inspections in 2013[26] and these changes were applied to all of the 2014 inspections. This is also in part due to the fact that some of the inspections this year were undertaken by an inspection team of three rather than two.

6.54 **Audits and query based searches.** My office has developed the interception audits over the last two years and they are now at a significantly more mature level. We have unfettered access to the application and authorisation systems in place within a number of the interception agencies and we examine the warrant documentation electronically rather than on paper. Where the interception agency also uses that system to evaluate the intercepted material (and related communications data) and produce intelligence reports we are able to conduct query based searches against the material and reports.

6.55 These searches give better insight into how the material has been used, enable specific areas to be tested for compliance, and allow trends and patterns to be identified from the extraction of information from large volumes of applications. Furthermore it enables us to examine within the operational environment the Article 8 interference actually being undertaken. In a scientific sense, we test the operational hypothesis set down in the initial application that was authorised. These are all important components when formally reviewing and reassessing the necessity and proportionality of the conduct authorised and compliance with the legislation and it is crucial to examine those arrangements.

6.56 This is because when an application for an interception warrant is submitted the proportionality and collateral intrusion considerations in particular are based at a certain point in time and, importantly, prior to any interference being undertaken. In our view, in practice, an additional and appropriate test as to whether something is, was or continues to be proportionate to the Article 8 interference undertaken can only be obtained by scrutinising the operational conduct carried out or, put another way, the downstream use of the material acquired, for example by examining:

- how the material has been used / analysed;
- whether the material was used for the stated or intended purpose;
- what actual interference or intrusion resulted and whether it was proportionate to the aim set out in the original authorisation;
- whether the conduct became disproportionate to what was foreseen at the point of authorisation and, importantly, why the operational team did not initiate the withdrawal of the authority;
- the retention, storage and destruction arrangements for material acquired; and
- whether any errors resulted from the interference or intrusion.

6.57 For example, my office might conduct a query based search to check that the intercepted material has been examined in a timely fashion, or to scrutinise the

26 See Paragraph 3.32 of my 2013 Annual Report

intelligence value / benefit of the interception to enable an assessment to be made as to whether the conduct remains necessary and proportionate. Another example might be to run query based searches on keywords (e.g. "solicitor", "legal") to identify cases where communications subject to legal privilege may have been intercepted and retained. My office is then able to check whether that material has been handled in accordance with the section 15 safeguards and the special procedures outlined in Chapter 3 of the code of practice. It is this post-authorisation or downstream audit of what is (or just as importantly what is not) being done with the material that brings more scrutiny and oversight to the process.

6.58 In a large number of instances we are conducting our audit between renewals and this enables us to reassess the necessity and proportionality of the conduct authorised and review whether the conduct was foreseen by the person authorising the interception. Through our observations we have in a number of cases recommended a warrant's modification, required changes to operational practice to safeguard privacy, required additional information to be provided to the Secretary of State straight away or at the point of next renewal, or recommended a warrant's cancellation.

6.59 This audit function is easily achievable with the majority of the law enforcement interception agencies as they hold the warrant documentation and the intelligence reports relating to the intercepted material on sterile systems (due to the requirement to separate interception related documentation and intelligence from other business areas which are subject to the disclosure provisions of the Criminal Procedure and Investigations Act (CPIA) 1996). The same is not the case for the intelligence agencies as their systems in general do not separate out intercepted material from other types of intelligence which of course we have no statutory function to oversee. Although we have already made arrangements to view the applications electronically in a number of the intelligence agencies, we continue to explore how we might bring about more scrutiny and oversight to other parts of the process by electronic means. At present we are requiring further information and reports to be provided to us during inspections and are also interviewing staff on these matters.

6.60 **Retention, Storage and Deletion.** In my last annual report I reported on the process undertaken to examine the interception agencies' systems and policies in relation to the retention, storage and destruction of intercepted material (and related communications data)[27].

6.61 In brief, I wrote to all interception agencies in August 2013 requiring them to provide my office with full and systematically organised information about the retention, storage and destruction of the product of interception, in every generic database in which intercepted material (and related communications data) is for a time stored. I asked 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*

27 See Paragraphs 3.48 to 3.57 of my 2013 Annual Report

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."

6.62 My office's investigation led to the interception agencies embarking on major reviews of the retention, storage and destruction of intercepted material (and related communications data). In a small number of cases the interception agencies had already started this process due to planned organisational or IT system changes. I discovered that every agency has a different view on what constitutes an appropriate retention period for material. Although it is not for me to dictate what that period should be, I am keen to ensure that retention periods are not arbitrary and that the policies governing this area are well considered and underpinned by evidence.

6.63 Although my office's investigation demonstrated that indiscriminate retention for long periods of unselected intercepted material (content) does not occur and 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, I reported that related communications data are in some instances retained for a variety of longer periods and that I had yet to satisfy myself fully that some of the retention periods were justified.

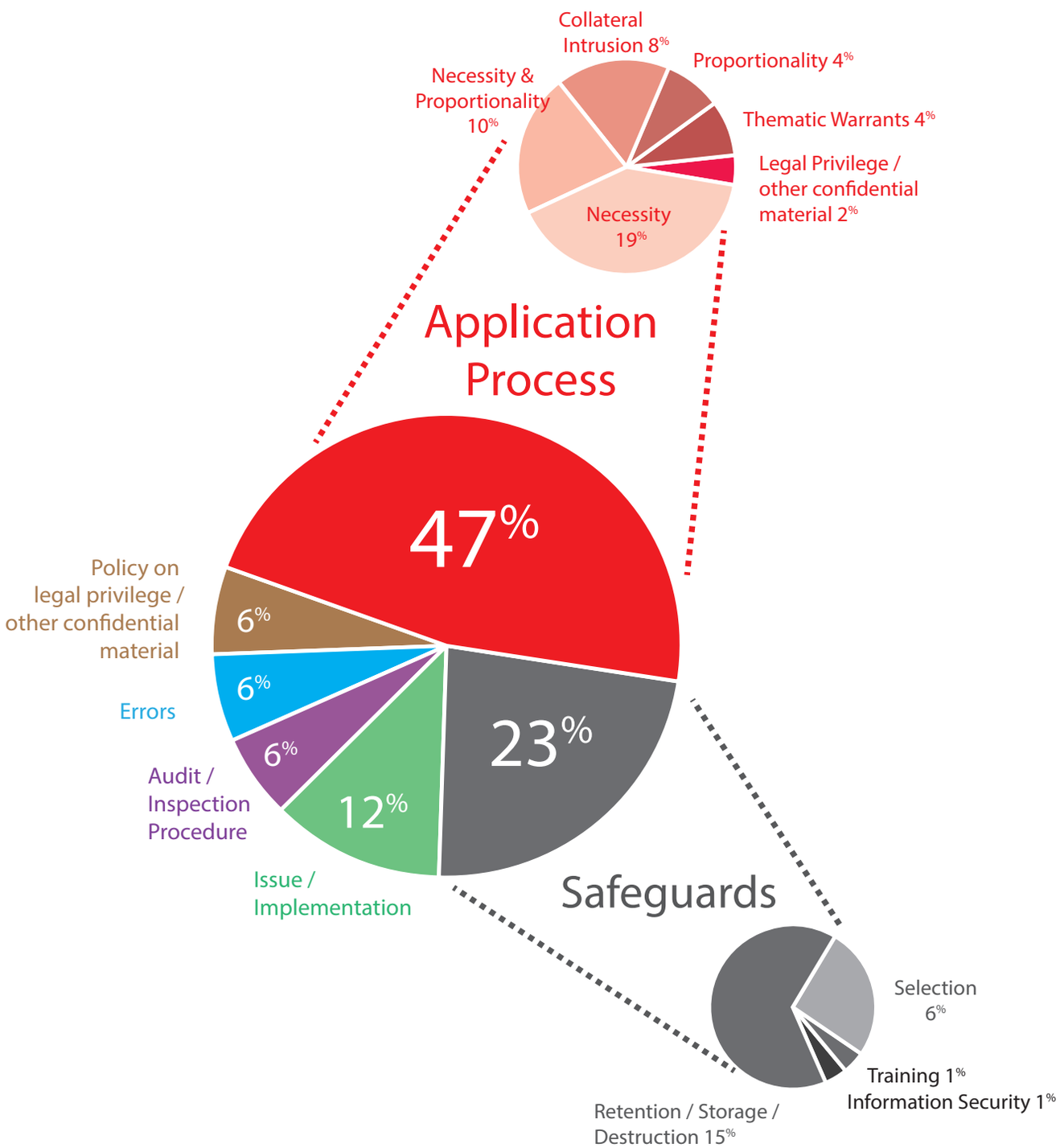
6.64 This investigation led my office to make 22 specific recommendations in 2013 and 11 specific recommendations in 2014 for the interception agencies to review or shorten their retention periods and/or destroy intercepted material and/or related communications data where there was no persuasive justification provided for its ongoing retention. A number of the 2014 recommendations were to ensure that the interception agencies remained focused on the issue, to boost their efforts to review their retention periods or destroy certain material, and to create a corporate culture of reviewing regularly and destroying material and data when it is no longer necessary and proportionate to retain it.

6.65 I can report that all of the recommendations were accepted by the interception agencies. The large majority have already been fully implemented. This has caused a significant amount of intercepted material and related communications data to be destroyed, and in some instances entire systems have been decommissioned. In other cases the maximum retention periods have been halved. Those agencies which have not yet managed to implement the recommendations in full are waiting on significant technical changes to be made to IT systems. I have made clear that future retention and destruction policies should not be dependent on broad assumptions about the value of the material or data. Reviews should be conducted regularly, informed by profiling exercises to ensure that the retention and destruction policies are not arbitrary. I welcome the progress made and my office will continue to monitor this area of the process.

Inspection Recommendations and Observations

6.66 The total number of recommendations made in our inspection reports for the 9 interception agencies was 69, an average of 8 per interception agency. We also, for the

Figure 3 *Interception Recommendations by Category*



first time, issued formal inspection reports to the WGDs in 2014 and 16 recommendations arose from the inspections of the 4 main WGDs.

6.67 Figure 3 shows that 82% of the recommendations made fell into 3 key categories: Application Process, Section 15/16 Safeguards and, Issue / Implementation of Warrants.

Application Process

6.68 47% of the recommendations were made in relation to the application process. The recommendations in this category can be broken into six distinct areas and some examples of the recommendations are given below.

6.69 **Necessity**. In a number of instances we challenged whether the interception met the statutory necessity grounds. A key part of the necessity test is to make the link between the individual under investigation, the communications address to be intercepted, and the serious crime or threat to national security. In a number of cases the link was not made between the first two points explicitly. In a small number of instances the warrant applications did not set out sufficiently what the specific interest / threat to national security was. It was unclear in a small number of cases how the crime under investigation met the 'serious' crime test set out in section 81(3), particularly where the interception had not produced any intelligence to substantiate the seriousness of the criminality. In a number of these cases there was other intelligence indicating that the individual was in fact engaged in serious criminality. As a result we required this information to be included in subsequent submissions, but directed that the interception agency should consider whether the conduct was still proportionate when balancing the value of the interception against the level of intrusion into the individual's privacy.

6.70 **Proportionality and collateral intrusion**. I have already touched on proportionality in the preceding paragraph and in the section where I discuss our downstream examination and query based searches. Because we are often conducting our audits while the interception warrants are still extant we are able to reassess proportionality by examining some of the intercepted material and interviewing relevant staff. In a number of the interception agencies we recommended that the applications must outline what steps would be put in place to minimise collateral intrusion, particularly where the communications addresses were likely to be used by individuals who were not of intelligence interest. Any renewal submissions should contain a considered assessment of the actual intrusion that has occurred (whether collateral or otherwise) and how effective the steps to minimise that intrusion have been. In a number of instances the renewals contained the same wording as the original submissions (i.e. they set out what intrusion was expected) when of course by that stage it was known what actual intrusion had resulted from the interception. We regarded this to be unsatisfactory.

6.71 **Thematic warrants.** Earlier in the report I made passing reference to so called thematic warrants. The term 'thematic' is not defined in statute but it is the name applied to section 8(1) warrants that are against more than one person. Section 81(1) specifies that *"person" includes any organisation and any association or combination of persons.* A

number of the interception agencies apply for 'thematic' warrants against clearly defined organisations or groupings of individuals where the case for necessity and proportionality can be met. For example, such a warrant might be appropriate in a fast moving and short term operation such as a kidnap or threat to life case or, in cases where there is reason to believe that a communications address is being used by a number of individuals belonging to an identifiable group.

6.72 On such warrants the description of the persons to be intercepted is broader and the particularities are then added by way of modifications. The Secretaries of State must be satisfied at the time they consider such warrants that the necessity and proportionality case is consistent and that the conduct is sufficiently foreseeable. There are examples where Secretaries of State have challenged thematic warrants and required individual warrants to be submitted, usually in cases where the individuals were all clearly identified. In a number of cases thematic warrants are also subject to more regular reviews at the request of the Secretary of State.

6.73 I considered the question of whether a so-called 'thematic' warrant could in theory comply with the law. I reached the conclusion that they could so long as they sufficiently name or describe the combination or association of persons. In a number of cases we have questioned however the strength of the association or combination of persons, or had concerns as to how each individual conformed to the description on the warrant instrument. We also raised concerns in a small number of cases that the specific proportionality considerations and collateral intrusion issues were not set out sufficiently for each individual. These concerns led to one of the interception agencies reviewing all of its thematic warrants. We also identified discrepancies in how the various interception agencies were using thematic warrants and recommended that a policy should be drafted and agreed by all interception agencies and WGDs setting out the key principles and circumstances under which it might be appropriate to use such warrants. This will result in increased consistency and compliance.

6.74 Thematic warrants are, at the moment, the exception rather than the rule. In fact a number of the interception agencies have yet to seek a thematic warrant. A case could be made however, that it would be appropriate to use thematic warrants more widely against, for example, a well-defined criminal or terrorist group working for a common purpose.

Section 15/16 Safeguards

6.75 23% of the recommendations were made in relation to the section 15/16 safeguards. The recommendations in this category can be broken into four distinct areas and some examples of the recommendations in the two main categories are given below.

6.76 **Selection.** My office made a recommendation relating to the content of the section 16(3) and (5) authorisations to ensure that it was always explicit when it became known that the individual was in the British Islands. Another recommendation was made to ensure that the justifications for selection were considered at the individual

communications address level as well as at the person level, particularly where there might be different collateral intrusion considerations. The remaining recommendations related to computerised safeguards, audits and authenticating reviews which have already been discussed earlier in this report.

6.77 **Retention, Storage and Destruction.** I have already provided significant detail on the nature of these recommendations in a preceding section of the report. In brief, specific recommendations were made for the interception agencies to review or shorten their retention periods and/or destroy intercepted material and/or related communications data where there was no persuasive justification provided for its continued retention.

Issue / Implementation

6.78 12% of the recommendations were made in relation to the issue or implementation of interception warrants. These included recommendations to improve the audit trail for those warrants issued orally under the direction of a Secretary of State, to reduce the pressure on interception agencies to renew warrants excessively early by introducing additional Secretary of State signing slots during recess periods, and to improve the timescales within which instruments, modifications and cancellations are served on CSPs.

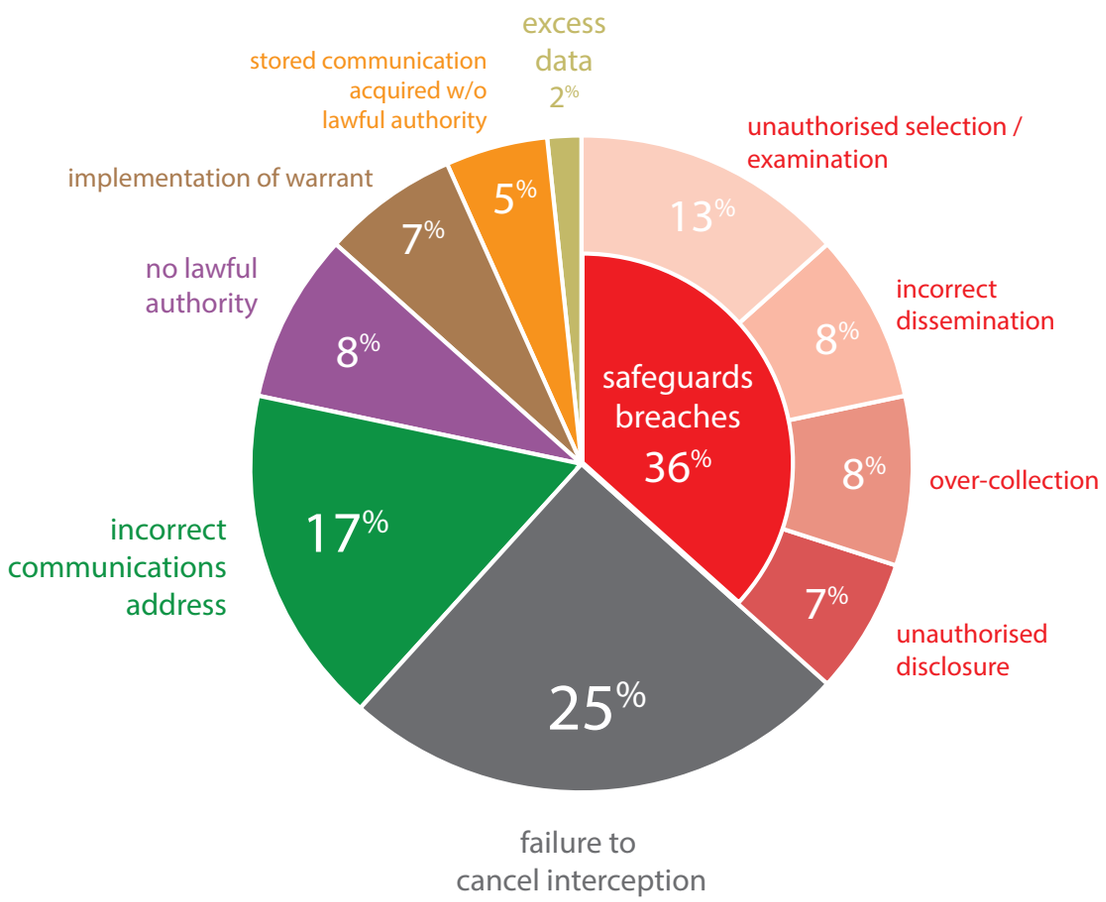
Summary of Recommendations & Observations

6.79 In 2014 my office made a number of recommendations in relation to the interception agencies' policies on legal privilege or otherwise confidential material. Chapter 3 of the interception code of practice contains guidance on this area. Furthermore I note the recent declaration by the IPT (following a concession by the Government) in relation to Belhadj & Others vs Security Service & Others, that since January 2010 the regime for the interception / obtaining, analysis, use, disclosure and destruction of legally privileged material has contravened Article 8 ECHR and was accordingly unlawful. The Respondents are now working with my office to review their policies and procedures to ensure that the safeguards are made sufficiently public and are compatible with ECHR. Furthermore at the time of drafting this report, a revised draft of the interception of communications code of practice is out for public consultation[28] and this sets out enhanced safeguards and provides more detail on the protections that must apply to privileged material. There is still the outstanding matter regarding whether the Claimants legally privileged communications have in fact been intercepted / obtained, analysed, used, disclosed or retained.

6.80 It will not be possible to judge progress against all of the 2014 recommendations until after the first round of the 2015 inspections. However, out of the 36 recommendations that were made in the first round of 2014 inspections, 30 had been fully achieved by the second round. The remaining 6 were accepted in full, but had not been fully achieved by the second round.

28 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf

Figure 4 *Breakdown of Interception Errors*



6.81 Through our audits we have in a number of specific cases recommended that interception warrants should be modified or cancelled, we have required changes to operational practices or procedures to safeguard privacy, or have required additional information to be provided to the Secretary of State or Senior Official in submissions. More broadly the recommendations made in relation to the application process have improved compliance and the clarity and quality of the necessity and proportionality justifications. Those made in relation to the section 15/16 safeguards have strengthened or tightened a number of the procedures for the retention, storage, dissemination and destruction of the intercepted material or related communications data.

Interception Errors

6.82 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 RIPA 2000, or any inadequate discharge of the section 15 safeguards.

6.83 In my 2013 report I noted that there was no provision for error reporting in the interception of communications code of practice, unlike the provision in the communications data code of practice. The interception agencies remain keen to report any instances which they judge to be errors, but their thresholds for reporting differed and there was a lack of consistency to the process. I am satisfied that progress has been made here.

6.84 In early 2014 my office convened a meeting with a number of the interception agencies to seek to establish a common understanding of what constitutes an error. Realistic case studies were used as a stimulus for discussion. These revealed some common ground, even though the agencies' operational challenges are often very different. My office has produced a draft memorandum of understanding as the basis for a robust error reporting system. We have tested this against the errors that were reported in 2014 to ensure that it is sufficiently comprehensive. This should provide a clear and consistent framework for error reporting.

6.85 In my 2013 report I mentioned concerns that some interception agencies delayed reporting errors until they had investigated the cause. This year my office has been provided with an early initial report of the error (or potential error) and a more detailed report once the investigation was complete. This is a welcome improvement which is codified in the memorandum of understanding.

Error Statistics

6.86 The total number of interception errors reported to my office during 2014 was 60, three more than in 2013. The breakdown of the causes of the errors is contained in Figure 4

6.87 55% of the errors were attributable to the interception agencies, 2% to the WGDs and 38% to the CSPs when giving effect to an interception warrant.

6.88 The remaining 5% of the interception errors were caused by CSPs providing police forces with the content of communications when they only required communications data under Chapter II of Part I, or, in one instance where a police force did not have the necessary authority in place to access stored communications[29]. It is important to make the point that this 5% did not relate to the issuing or implementation of interception warrants.

29 See section 1(5)(c), 2(7) and 2(8) of RIPA 2000

6.89 Figure 4 shows that 78% of the errors reported fell into 3 key categories: Section 15/16 safeguards breaches; failure to cancel interception; or interception of the incorrect communications address.

Section 15/16 safeguards breaches.

6.90 36% of the errors constituted breaches of the section 15/16 safeguards. The errors in this category can be broken down into four distinct areas and some examples of the errors are provided here.

6.91 **Over-collection.** These were technical software or hardware errors that caused over-collection of intercepted material and related communications data. Where errors are caused by a single technical fault there may be multiple consequences (i.e. large volumes of material erroneously collected). In some of these cases the material and data contained details of individuals' private communications, whereas in other cases the material contained communications that were not personal in nature. These errors can take a number of months to investigate and generally the cause of the error or system malfunction is identified and completely resolved. A significant amount of work is undertaken to implement measures to prevent recurrence and, in some cases periodic sampling and checking procedures were implemented to enhance the interception agency's ability to monitor and detect such errors. In all cases steps are taken immediately to ensure that the erroneous material and data is deleted.

6.92 **Unauthorised selection / examination.** One example of an error in this category is where an analyst had mistakenly continued to select the communications of an individual based overseas after the individual was known to have entered the United Kingdom. In one very serious case last year an employee at GCHQ deliberately undertook a number of unauthorised searches for related communications data. The employee was immediately suspended from duty on discovery of the illegitimate searches and a full investigation was launched. This abuse of the systems amounted to gross misconduct and the individual's employment was terminated and vetting status withdrawn. Given the actions undertaken, i.e. that the individual accessed GCHQ's computers for an unauthorised purpose, it is arguable that an offence under section 1 of the Computer Misuse Act was also committed. This is the first known instance of deliberate abuse of GCHQ's interception and communications data systems in this way.

6.93 **Unauthorised disclosure.** These error instances constitute non-compliance with section 15(2) of RIPA 2000. They were caused by the interception agency not limiting the number of persons to whom (or the extent to which) any of the material or data was disclosed or otherwise made available to the minimum that was necessary for the authorised purpose. For example, in a small number of cases intercepted material or the fact of the existence of an interception warrant was disclosed to additional persons within an interception agency or to persons outside of an interception agency.

6.94 **Incorrect dissemination.** These error instances also constitute non-compliance with section 15(2) of RIPA 2000. They were caused by CSPs misdirecting the intercepted

material and related communications data to the incorrect interception agency. In all cases the mistake was identified by the receiving agency immediately (as their technical systems were not expecting that particular product) and the material and data received erroneously was deleted.

Failure to cancel interception.

6.95 25% of the errors were caused by a failure to cancel interception. These were in the main caused by staff in the interception agency or CSP failing to effect the cancellation properly on technical systems. Because the interception is effected technically at both ends (i.e. at the CSP and at the interception agency), if the CSP fails in its duty no significant intrusion generally results as the material is stopped from entering the interception agency or is immediately discovered by system administrators and deleted.

Incorrect communications address intercepted.

6.96 17% of the errors were caused as a result of the incorrect communications address being intercepted. The majority of these errors are human in nature. In some instances the interception agency applied for the warrant in good faith on information received from a third party, but the information turned out to be wrong due to a transposition or other mistake in the reporting. In these cases 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 or communications address intercepted did not in the end relate to the individual of interest. In 2013 I directed that these errors should be reported to my office where product had been obtained as, even though the warrant was authorised in accordance with the law, the conduct resulted in an unintentional invasion of privacy. In other cases there was an inadvertent transposition of the communications address by the interception agency when applying for the warrant or by the CSP when effecting the interception. In the majority of cases the staff conducting the interception detected these errors promptly and the interception was immediately suspended and then cancelled. In all cases the erroneous material and data was deleted.

6.97 In all cases the interception agencies and CSPs provided my office with full reports of the errors, the necessary investigations were carried out to ensure that the measures put in place to prevent recurrence were sufficiently robust, and that any erroneously acquired material or data was destroyed. Technical system errors are challenging and remain a cause for concern. Technical system errors have been particularly prevalent in the communications data area of our oversight which is of concern. This is discussed in Section 7 of this report.

Points of Note

Interception of Communications

2795 interception warrants (to access the content of communications and related communications data) were authorised in 2014 , an increase of 1.3% on the previous year.

1605 interception warrants were extant on 31st December 2014. Of those, 20 were issued under section 8(4).

In 2014 my office conducted 26 interception inspections. During these inspections 936 interception warrants were examined which equates to 58% of the number of extant warrants at the end of the year or 34% of the new warrants issued in 2014.

The total number of recommendations made in our inspection reports for the 9 interception agencies and 4 warrant granting departments was 85. The audits undertaken by my office and resultant recommendations have lead to improved compliance in key areas or systems and procedures to be changed to enhance safeguards.

In 2013 I made a number of recommendations about the retention, storage and destruction of intercepted material and related communications data. A large majority of these recommendations have now been implemented in full which has resulted in a significant amount of material and data being destroyed and retention periods being reduced where there was no persuasive justification provided for its ongoing retention.

60 interception errors were reported to my office in 2014. 78% of the errors fell into three main categories: section 15/16 safeguards breaches; failure to cancel interception; or interception of the incorrect communications address. The interception agencies and Communication Service Providers (CSPs) provided my office with the full details of these errors, the consequences were investigated, steps were taken to prevent recurrence and any erroneously acquired material or data was destroyed.

Overall our experience is that the interception agencies have a desire to comply with the legislation and to achieve high standards in the work that they carry out. There is a strong culture of compliance and of self reporting when things go wrong. There is however always room for improvement and the work that my office undertakes assists the interception agencies to keep their systems and their use of these intrusive powers under constant review.

Section 7
Communications Data

7.1 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 and some of the inquiries my office has undertaken in the reporting year.

Types of Communications Data

7.2 Chapter II of Part I (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).

7.3 The definition of communications data has not changed since RIPA 2000 came into existence, despite the fact that communications technologies, and thus the types of information generated and processed have changed dramatically.

7.4 Section 81(1) of RIPA 2000 defines a communication to include anything comprising of speech, music, sounds, visual images or data of any description. It also includes the movement of those communications between persons, a person and a thing or between things. So, that would include an end-user downloading music from a website and sharing it with other users via a telecommunication system. It also includes the actuation or control of another apparatus within a telecommunication system for example, activating storage from one device to another device via a telecommunication system.

7.5 In practice users will often access several telecommunication services via their mobile phone and those services are unlikely to be supplied by the CSP who provides their network connection. Put simply, service use and traffic data are the data generated

and processed by the CSP who provides network access; and other providers of telecommunication services accessed via a network connection.

7.6 The definitions of service use and traffic data (see sections 21(4)(a), (b) and 21(6)) are, in our view, still generally fit for purpose, albeit they can be difficult to understand without proper explanation especially when considering the developments in communications technology since the RIP Bill was debated. The volumes and detail contained, especially in traffic data, are at a level not envisaged in 2000. The introduction of mobile phone networks with capacity to be able to provide access to radio & television channels, social networking and other services is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone / end user device. The amount of information collected by the provider of a communications service about the people to whom they provide a service has also increased considerably and this means that the definition of "subscriber information" potentially now covers a wider catchment of data than originally available. Furthermore it is sometimes difficult to determine what constitutes the content of a communication within the online environment. RIPA 2000 refers to content several times but content itself is never defined. In December 2014 my office published our submission to the Investigatory Powers Review[30] and this explains some of the pressing issues in this regard.

Applications for Communications Data

7.7 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),

7.8 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) as amended[31].

7.9 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. There is huge variance in the extent to which these powers are utilised by the different public authorities. Only one quarter

30 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

31 http://www.legislation.gov.uk/uksi - Statutory Instruments (SIs) 2011/2085, 2012/2007, 2013/472, 2013/602, 2014/549, 2015/228

of the public authorities with powers to acquire data actually used their powers during 2014, which is a lower proportion than in 2013 (approximately one third).

7.10 40% of the public authorities that have powers to acquire communications data have never used their powers.

7.11 13 public authorities have recently had their powers removed. 4 of these had never used their powers, and the remaining 9 collectively approved 103 applications for communications data in 2014.

7.12 The giving of lawful authority for acquiring communications data is set out in the statute and is undertaken by a 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 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 of practice. 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 of practice – see in particular the list of functions in paragraph 3.17. These include:
  - advising both applicants and DPs on the interpretation of Chapter II of Part I RIPA 2000, 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 RIPA 2000.
- 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 Chapter II of Part I RIPA 2000 and the code of practice.

7.13 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.

7.14 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.

7.15 **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 so far as those interests are also relevant to the interests of national security;
- 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 and The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015 (SI No. 228) for these.

7.16 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."

7.17 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.

7.18 **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.

7.19 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

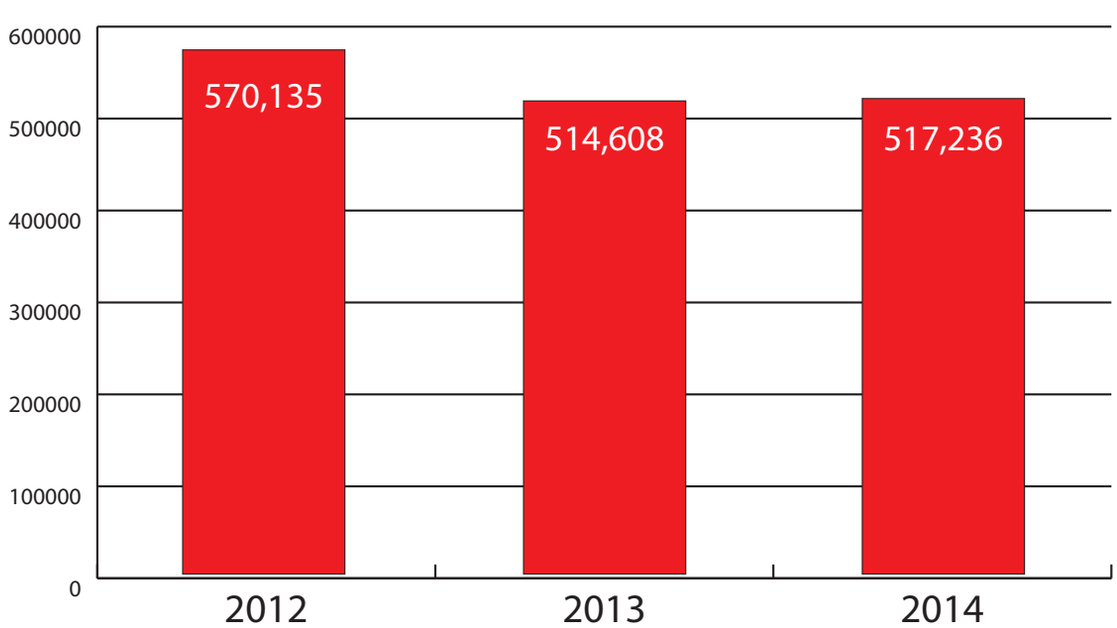
be obtained by other less intrusive means. Applications for communications data are refused (or not applied for) where it is judged that the necessity does not outweigh the intrusion. For example, an application is more likely to be granted for a mobile telephone which a suspect is known to use for criminal purposes than if the telephone may also be used by other members of the individual's family as well. In such cases the acquisition of unconnected and intrusive data might be unavoidable. Judging the likely intrusion in advance is not an exact science.

Statistics for Communications Data

7.20 My office has previously referred to the inadequacy of the statistical requirements in the Acquisition and Disclosure of Communications Data code of practice. The Home Office recently included a more comprehensive set of statistical requirements in the amended draft code of practice[32]. These new requirements will improve transparency and provide for more meaningful analysis. Public authorities are currently working to ensure their recording systems are amended to fulfil the new statistical requirements from April 1st 2015, including the ability to capture information not previously recorded.

7.21 Figure 5 shows the number of authorisations and notices for communications data over the previous three years (excluding urgent oral applications). The total number

Figure 5 *2012-2014 Total Authorisations & Notices under Chapter II of Part I RIPA 2000 (ex urgent oral applications)*



32 https://www.gov.uk/government/publications/communications-data-draft-codes-of-practice-acquisition-disclosure-and-retention

issued or granted in 2014 was 517,236 which although higher than the previous year, does not represent a significant increase.

7.22 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 2014 there were 55,346 notices and authorisations given orally. This represents an increase on the 42,293 notices and authorisations given orally in 2013. Our inspections have identified that much of this increase is due to the police providing an enhanced emergency response to trace missing children at risk of sexual exploitation. I note that the draft code of practice has clarified that the section 22(2)(g) statutory purpose[33] may be used in circumstances where there is serious concern for the welfare of a vulnerable person.

7.23 Annex B of this report provides a breakdown of the 517,236 notices and authorisations by public authority. The number of notices given and authorisations granted by public authorities is only indicative of the amount of communications data acquired and must be treated with caution for the reasons I outlined in paragraph 4.19 of my 2013 Annual Report. Essentially it would be inappropriate to draw comparisons between the public authorities as they apply different counting mechanisms and rules. It is important therefore that the numbers are not used to produce league table comparisons.

7.24 The new statistical requirements in the amended draft code of practice will require public authorities to record the number of applications for communications data and the individual items of data requested. The latter of which should be a more meaningful figure than the number of authorisations and notices. It is also likely to be higher. In November 2014 my office published a diagram to assist understanding as to the relationship and ratio between the number of notices & authorisations and applications[34]. Our estimate at that time was that the ratio was an average of 2.5:1 notices & authorisations to applications.

7.25 This year I used my power under section 58(1) of RIPA 2000 to require public authorities to collate the number of applications for communications data that were approved. Previously my office had only been able to estimate this statistic from limited data sets. In total there were 267,373 applications and so the actual ratio of notices & authorisations to applications in 2014 was 2:1.

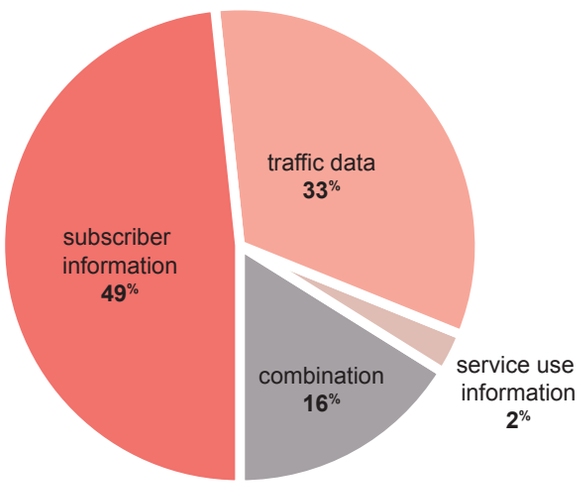
7.26 Figure 6 shows the breakdown of notices and authorisations by type of data under section 21(4). Almost half of the requirements were for subscriber information under section 21(4)(c). The breakdown is much the same as for 2012 and 2013.

7.27 Figure 7 shows the breakdown of the 517,236 notices and authorisations by type of public authority. 88.9% of these were made by police forces and law enforcement

33 RIPA 2000 s.22(g) 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;

34 http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf

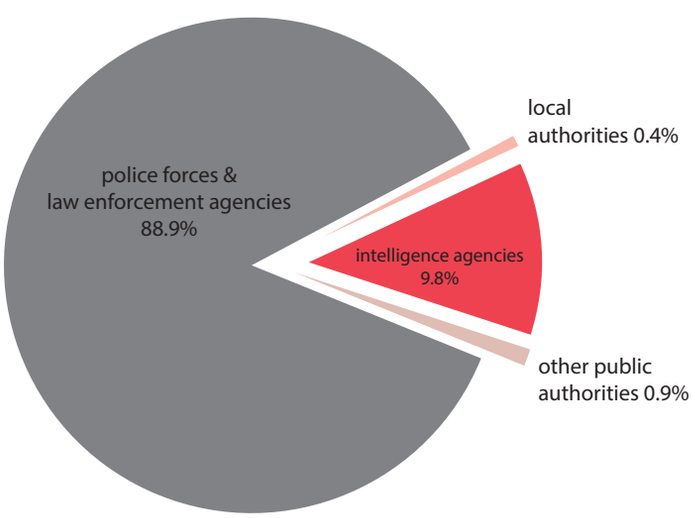
Figure 6 *2014 RIPA 2000 Part I Chapter II Authorisations & Notices by Data Type*



agencies. Less than 2% 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. Of particular note is that no Fire & Rescue Authorities or Ambulance Trusts reported using their powers in 2014. Just over a fifth of Local Authorities reported using their powers in 2014.

7.28 Finally, this year my office repeated an exercise conducted for my 2013 Annual Report to provide some further statistical information in relation to the statutory necessity purposes under which data is required in order to better inform the public about how

Figure 7 *Chapter II of Part I RIPA 2000 Authorisations & Notices by Public Authority Type (2014)*



the powers are being used. This statistic is particularly important as 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. Figure 8 shows that just half a percent of all the requests were for purposes other than the prevention and detection of crime or the prevention of disorder, in the interests of national security, or in an emergency to prevent death or injury. Figure 8 also reiterates the point I have made elsewhere[35] that it is inaccurate and unhelpful to refer to RIPA 2000 as anti-terrorist legislation and infer that its use for non-terrorist related matters is inappropriate.

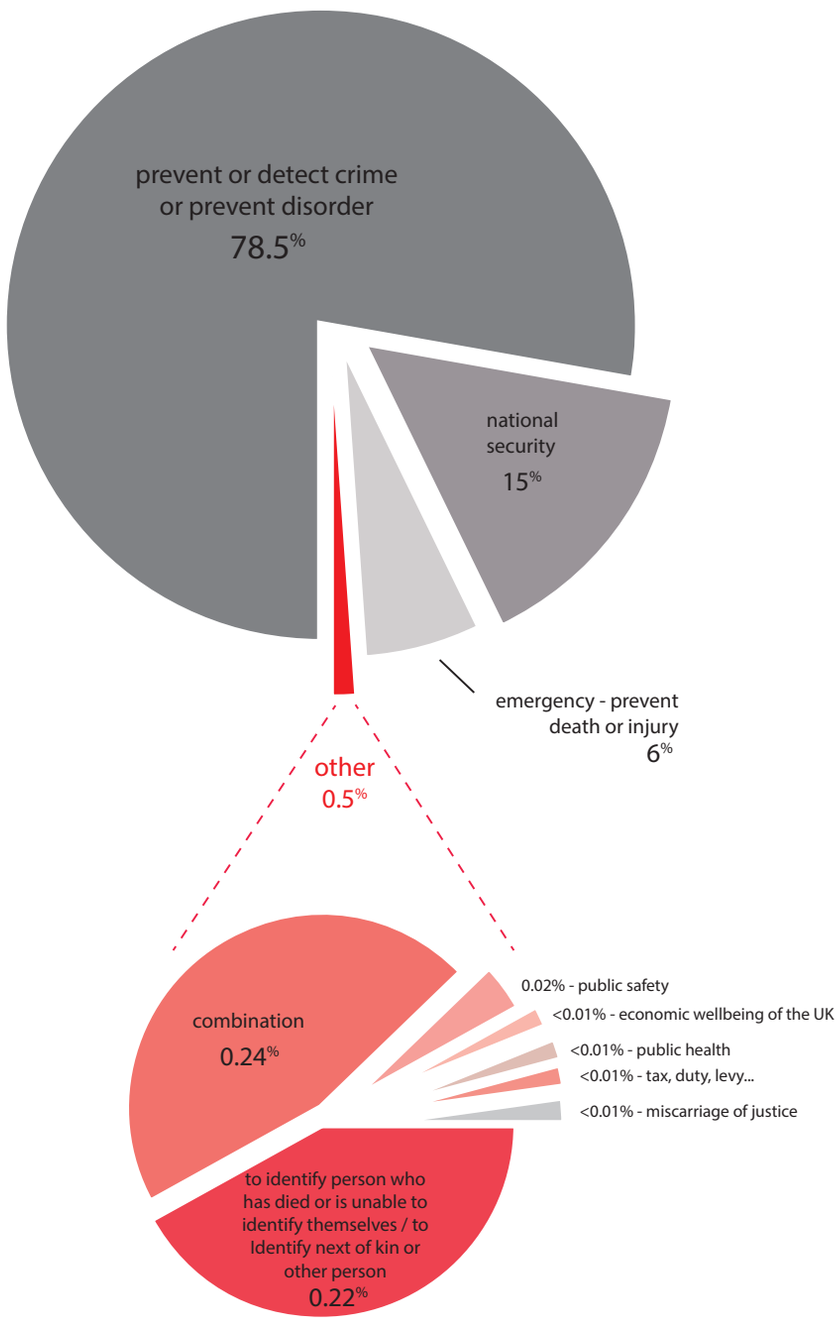
7.29 It is not possible to report the number of individuals to whom the 517,236 notices and authorisations relate. What we can say is that number would be much smaller as public authorities often make multiple requests for communications data in the course of a single investigation, and also make multiple requests for communications data in relation to the same individual. We note that the Home Office has not included a requirement for this statistic to be collected in the revised code of practice.

7.30 Although this would undoubtedly be an informative statistic, in our view there are a number of compelling reasons as to why the collection of this statistic is likely to be prohibitively difficult. For example, one notice or authorisation may include data requirements that relate to different individuals; there is not always a one-to-one relationship between a communications address and an individual; a large number of requests are unsuccessful in conclusively attributing a communications address to an individual; there would be duplicates for a number of reasons, for example, different police forces might be investigating and acquiring data on the same individuals (and even when those individuals had been identified those requests might not be linked). Furthermore the statistics that are currently collected by public authorities are all recorded at the start of the process or at the point of requesting the data. At this point of the process the individual on whom data is being acquired is often unknown, and this might well be the reason why the data is being acquired in the first place (i.e. to identify an unknown individual).

7.31 The best chance therefore of comprehensively attributing communications addresses to individuals would be at the termination of an investigation where various sources of information in addition to communications data could be drawn upon. But even at the end of the investigation there might still be a large degree of ambiguity or a number of communications addresses that have not been attributed successfully because it was not possible to do so or, because it was no longer a relevant line of inquiry to pursue and therefore it was not appropriate for the public authority to identify to whom the particular communications address relates to. Such retrospective recording of information would represent a major shift from the current statistical recording practices and, in our view, would be an onerous administrative burden. My office would also be concerned about the unintended consequence whereby a greater amount of communications data might be sought than was actually necessary in order to satisfy the statistical requirements of linking a communications address to an individual. This year during our operational reviews, which we will discuss later in this section of the report,

35 http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

Figure 8 *2014 Chapter II of Part I RIPA 2000 Applications by Statutory Purpose*



Caveat: This chart is created to give indicative proportions of which statutory purpose the approved applications in 2014 were for. It is indiciative because a small minority of police forces were unable to provide an accurate breakdown. Their contribution to the total has been extrapolated from the majority of police forces that were able to give an accurate breakdown.

my office collected statistics in relation to whether the data that was acquired related to a suspect, victim, witness or other category of individual, and this more achievable statistic goes some way to better inform the public about how the powers are being used. I note that the Home Office has included this statistical requirement in the revised code of practice.

Inspection Regime

7.32 My office's communications data inspections are structured to ensure that key areas derived from Chapter II of Part I of RIPA 2000 and the code of practice are scrutinised. A typical inspection may include the following:

- the supply of a pre-inspection pack (two months prior to our visit) to the head of the public authority to require information and arrange interviews with operational teams;
- a review of the action points or recommendations from the previous inspection and their implementation;
- 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;
- random 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;
- query based examination of applications, via interrogation of the secure auditable computer systems used by the larger public authorities, to identify trends, patterns and compliance issues in key parts of the process across large volumes of applications;
- 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; and,
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant public authority, i.e. the Chief Constable or Chief Executive.

7.33 **Number of inspections.** In 2014 my office conducted 90 communications data inspections broken down as follows: 51 police force and law enforcement agency, 3 intelligence agency, 18 local authority and 18 'other' public authority inspections. In 2014 my office moved to conduct annual inspections of the public authorities that acquire

larger volumes of communications data and this accounts for the increased number of inspections in 2014.

7.34 An additional 102 local authorities were inspected during the National Anti Fraud Network (NAFN) inspection. NAFN continues to provide a SPoC service for local authorities and over 90% of the local authorities that reported using their powers in 2014 submitted their requirements via the NAFN SPoC. NAFN continues to achieve a good level of compliance with RIPA 2000. On 1st December 2014 the Home Office prescribed that all local authorities must submit their communications data requirements via the NAFN SPoC.

7.35 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.

7.36 **Samples.** I have previously said 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 as important as scrutinising yet more individual applications. This is also in line with what Parliament intended, i.e. that the Interception Commissioner would *"check what is happening in practice, rather than examine every case universally."*[36] In the smaller public authorities it is usually feasible for my inspectors to examine all of the applications submitted in the period being examined. For the larger volume users sampling must be undertaken. We conduct two types of sampling, random sampling where the application process is examined from start to end, and query based searches where key parts of the process are scrutinised. In 2014 my inspectors scrutinised at random approximately 13,000 applications during the 90 inspections and nearly 100,000 applications were subject to query based searches.

7.37 It is 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 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.

36 Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill Comments by the Minister of State, Home Office (Mr. Charles Clarke)

7.38 **Query based searches.** My office has direct engagement with the software companies that supply secure auditable systems for administering communications data applications in the majority of the police forces and law enforcement agencies (who between them account for nearly 90% of the communications data requests). The software companies have developed capabilities to enable my office to retrieve data by means of query based searches relating to the applications so as to give better insight into all of the activities undertaken by an authority. This enables specific areas to be tested for compliance, and, trends and patterns to be identified from the extraction of information from large volumes of applications, for example:

- extraction of named DP and their recorded considerations for each application to check they are discharging their statutory duties responsibly, i.e. that they are not rubber stamping applications, that they are of the appropriate rank or level to act in that capacity, that they are independent of the investigation or operation;
- requests where service use or traffic data has been applied for over lengthy time periods to check relevance and proportionality;
- the acquisition of particularly intrusive data sets to examine the proportionality and intrusion considerations balanced against the necessity.

7.39 Furthermore it enables us to examine within the operational environment the interference actually being undertaken. When an application for communications data is submitted the proportionality and collateral intrusion considerations in particular are based at a certain point in time and, importantly, prior to any interference being undertaken. In our view, in practice, an additional and appropriate test as to whether something is, was or continues to be proportionate to the interference undertaken can only be obtained by scrutinising the operational conduct carried out or, put another way, the downstream use of the material acquired, for example by examining:

- how the material has been used / analysed;
- whether the material was used for the stated or intended purpose;
- what actual interference or intrusion resulted and whether it was proportionate to the aim set out in the original authorisation;
- whether the conduct become disproportionate to what was foreseen at the point of authorisation and in instances where future data is being acquired why the operational team did not initiate the withdrawal of the authority; and
- whether any errors / breaches resulted from the interference or intrusion.
- in a scientific sense, we test the operational hypothesis set down in the initial application that was authorised.

7.40 **Inspection Reports.** The reports contain a review of compliance against a strict set of baselines that derive from Chapter II of Part I 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.

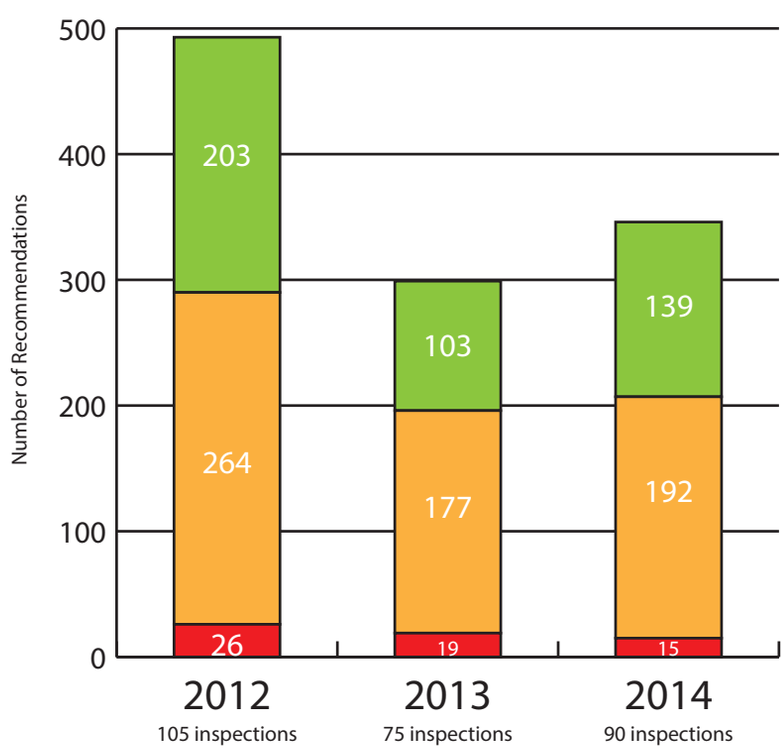
Inspection Findings & Recommendations

7.41 Inspection Findings and Recommendations. The total number of recommendations made during our 90 communications data inspections in 2014 was 346 (Figure 9). 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 Chapter II of Part I RIPA 2000 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.

7.42 This year 15 (4.3%) of the recommendations were red, 192 (55.5%) amber and 139 (40.2%) 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

Figure 9 *Total Red, Amber & Green recommendations resulting from communications data inspections 2012-2014*



	2012	2013	2014
Average no. of recommendations per inspection	4.7	4.0	3.8

differs. However, in 2014 the inspectors made on average fewer recommendations per inspection than in 2013 & 2012. The proportions of red, amber, green have remained broadly the same.

7.43 Figure 10 shows the breakdown of the 2014 recommendations by category. Just over half of the recommendations fell into 3 key categories:

Applicant.

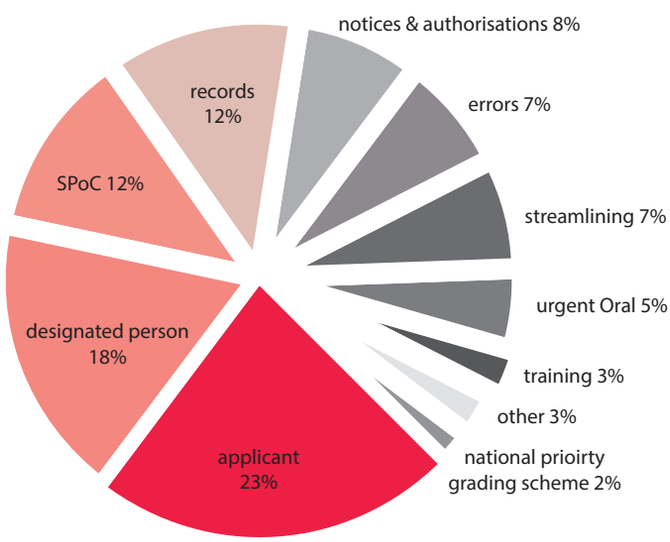
7.44 The majority of the recommendations in this category focused on the necessity or proportionality justifications set out by the applicants. The inspectors made recommendations relating to these two principles in approximately half of the public authorities inspected as they were not satisfied that they had been sufficiently justified in all of the applications that were examined.

7.45 For example there were instances where it was not clear how the requirement met the section 22(2) necessity test as the criminal offence/s under investigation had not been clearly set out in the application or, where the data required did not appear to be a proportionate response to the matter under investigation as the time period over which the data was acquired appeared to be excessive or because the applicant had not set out the objective of acquiring the data. In such instances the inspectors will seek further supporting documentation (such as case files, policy logs etc.) or will interview the applicant or DP. On the basis of this further information the inspector is normal able to satisfy themselves that the requirements were a necessary and a proportionate response, but that the application was not properly constructed. On occasions the inspectors noted that applicants included lengthy extracts of unnecessary or irrelevant information in their necessity and proportionality justifications to the point that the text totally detracted from what the application was about. This practice makes it harder for the SPoC and the DP to focus on the key issues that are relevant to the specific data request and the individual to whom it relates. In essence, efforts to submit large quantities of text do not add to the legitimacy of the requirements and the justifications can become opaque to the point that the ECHR considerations cannot be easily considered. These issues did not affect all applications submitted by those public authorities who received recommendations in this area; however they were prevalent enough across the samples examined for the inspectors to consider that recommendations were necessary.

Single Point of Contact (SPoC).

7.46 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 certain key areas, or, to improve their efficiency in approximately one third of the inspections.

Figure 10 *Communications Data - 2014 Inspection Recommendations by Category*



7.47 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. Although not complete, statistical information obtained by our office indicates that approximately 20% of applications are returned to the applicants by the SPoC for development or improvement.

7.48 As was the case in 2013, our inspections in 2014 also identified that a small number of SPoCs were experiencing serious backlogs in dealing with applications due to a lack of staff or inadequate systems. 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 takes weeks to process an application. My inspectors also made a number of good practice (green) recommendations on how efficiency might be improved within a SPoC e.g. for SPoCs to engage more proactively with applicants to ascertain the data that is required to fulfil their objective and ensure that the conduct is not arbitrary or excessive in the circumstances.

Designated Persons (DPs).

7.49 The inspectors made recommendations in relation to the role being performed by DPs in nearly half of the inspections undertaken. The majority of the recommendations in this category fell into two key areas; DP considerations and DP independence.

7.50 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. 5% of applications were rejected or returned for redevelopment by the DPs.

7.51 The inspectors concluded that the vast majority of DPs were completing their written considerations to a good or satisfactory standard. Where satisfactory, the inspectors highlighted to DPs, as a matter of good practice, how they could further improve their considerations e.g. by avoiding the use of generic phrases within their written considerations and ensuring that comments are tailored to the individual applications being considered.

7.52 The inspectors raised concerns with regard to the level of independence of the DPs in a number of public authorities and made recommendations to ensure that DPs who are directly involved in investigations do not consider applications.

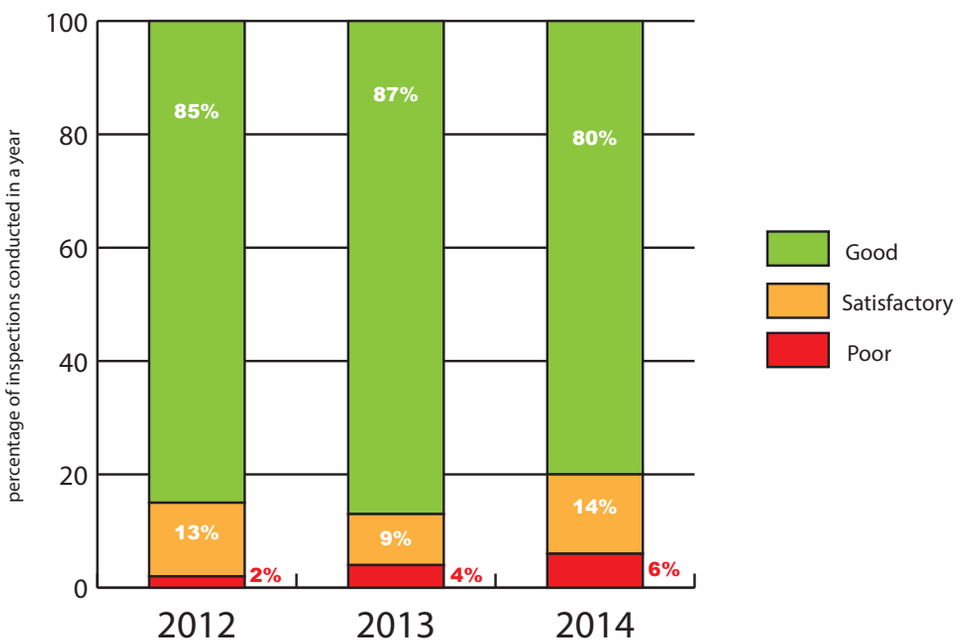
7.53 In comparison to the previous year the proportional breakdown of recommendations in 2014 is very similar. The number of recommendations in the record keeping and errors categories has increased. The recommendations in relation to record keeping were varied due to the different systems and recording practices utilised in public authorities. A number related to ensuring that the contemporaneous records are sufficiently completed when making use of the urgent oral process and, a number concerned the updating of workflow systems and processes to provide more reliable statistics or to better facilitate inspections by IOCCO. With regard to the Errors category the greater proportion can be explained by my office recommending that steps needed to be taken to reduce human transposition errors by, for example, enabling communications addresses to be 'copied and pasted' from the source documentation to the application and acquisition system. I will say more about this latter point in the Errors part of this section.

7.54 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. The proportion of inspections given an overall rating of good dropped to 80% from 87% in 2013 (Figure 11). As previously stated it is difficult to compare previous years because the public authorities inspected each year change.

7.55 A more reliable way to gauge whether compliance is improving is to compare a public authorities rating in 2014 to the rating from its previous inspection. In 2014 79 of the 90 public authorities inspected had been subject to an inspection in preceding years. 62 of the 79 public authorities maintained their level of compliance at either satisfactory or good; 6 improved and emerged with a good level of compliance when they had previously only achieved a satisfactory rating; and the remaining 11 public authorities worsened moving from good to satisfactory or, in two instances moving from a good to a poor level of compliance.

7.56 76 of the 90 public authorities inspected in 2014 had received recommendations

Figure 11 *Communications Data - Inspection Ratings 2012-2014*



in their previous inspection. 62% of those public authorities fully achieved all of their recommendations; 37% achieved the majority; and in the remaining one case only a minority of recommendations had been achieved. My office scheduled to re-inspect that public authority as a matter of priority.

7.57 In 2014, 37 of the recommendations had persisted, in that they were given to the public authority in a previous inspection, but had not been addressed. These persistent recommendations were for a wide range of issues, consistent with the proportions identified overall (Figure 10). I am therefore unable to conclude that public authorities have greater difficulty implementing some of our recommendations, compared to others.

Inquiries into Specific Issues

7.58 Last year my office conducted a number of inquiries which concentrated on examining certain areas of the process during inspections or, in one instance, investigating a matter about which there was significant public concern. This section of my report provides the details of these inquiries.

Inquiry into whether there is significant institutional overuse of Chapter II of Part I RIPA 2000 powers by police forces and law enforcement agencies

7.59 In my 2013 Annual Report I raised a question of concern about whether there might be significant institutional overuse of the powers. I was concerned 514,608 notices and authorisations was, at face value, a very large number, and accordingly asked my inspectors to investigate. On the basis that police forces and law enforcement agencies account for nearly 90% of notices and authorisations I was in particular interested in whether 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. The total number of authorisations and notices for 2014 (517,236) is similar to the 2013 figure and the police forces and law enforcement agencies again account for nearly 90% of the usage.

7.60 I made the point that I did not consider that this matter could properly be scrutinised by looking only at individual requests, which, taken alone, may be entirely justified, and that it would be necessary to take a broader view of institutional assumptions and use. Accordingly, in 2014 my inspectors undertook a number of operational reviews as part of their normal inspection regime. These are discussed in greater detail below.

7.61 My office required all of the larger volume communications data users being inspected to provide the details of all operations within the previous 12 months where more than 10 applications for communications data were submitted. The inspectors selected one or two operations at random within each public authority to review in detail and assess whether the acquisition of the data was as a whole a proportionate response. They undertook the reviews by examining all of the applications relating to the operation, associated documents such as communications data strategies, case summaries, policy logs and analytical reports. They then conducted interviews with key staff (e.g. the senior investigating officer, applicant, the lead investigator, analyst etc) to explore further whether the data requirement was a proportionate response and test whether the material was used for the stated or intended purpose and whether the actual interference was proportionate to the aim.

7.62 In 2014 my office scrutinised 54 operations as part of this inquiry. Those 54 operations submitted 2600 applications between them, an average of 48 applications per operation. A breakdown of the types of investigations examined is provided in Figure 12.

7.63 Overall, 80% of the data acquired in these operations related to suspects. 6% related to victims, 3% to witnesses and the remaining 11% to associates of the suspect or victim where it was to be determined if they were themselves suspects or witnesses.

7.64 The inspectors found that in each operation the communications data requirement was, overall, necessary and proportionate to the matter under investigation and no evidence of significant institutional overuse was found. However, in about a quarter of the operations the inspectors had to seek further information from the investigating officers or applicants to satisfy themselves that this was the case. This was principally

the result of poorly completed applications where applicants had failed to articulate, for example:

- how a specific suspect was linked to the offence being investigated;
- the credibility of the information linking a suspect to an offence;
- the objective for acquiring data on those who appeared to be peripheral witnesses or associates;
- how the periods of data sought were relevant to pertinent events; or,
- how the particular data set being requested linked to a specific investigative objective.

Figure 12 *Operational Reviews - Investigation Type*

Type of Investigation	No. of operations examined
Murder (inc. attempt murder)	15
Drugs Supply	7
Robbery	7
Sexual Offences	5
Burglary (inc. aggravated burglary)	5
Human Trafficking / Slavery	4
Fraud	3
Prevention of terrorism	2
Kidnap	2
Theft	2
Misconduct in public office	1
Firearms	1

7.65 My inspectors identified that communications data was frequently relied on to provide both inculpatory and exculpatory evidence. The communications data acquired revealed suspects movements and tied them to crime scenes. It often led to other key evidence being identified or retrieved. Links to previously unidentified offenders and offences were revealed. Dangerous offenders were located and offences were disrupted with the assistance of communications data. Patterns of communication provided evidence of conspiracy between suspects. The data highlighted inconsistencies in accounts given by suspects and corroborated the testimony of victims. The data determined the last known whereabouts of victims and persons they had been in contact with. Similarly, communications data assisted to eliminate key suspects or highlighted inconsistencies in accounts given by victims.

7.66 In a couple of the operations examined the inspectors concluded that there were potentially gaps in the acquisition process where the investigation teams had not identified the full range of data necessary to achieve the objective. This failure to identify relevant data may adversely impact on the ability to, for example, corroborate the account given by a witness, corroborate the testimony and / or determine the last known whereabouts of a victim or properly determine the role of a suspect in a crime or indicate their innocence. This may present the acquisition process as arbitrary and serious implications could result. This is an area in which it is important for the SPOCs to engage with the applicants to develop strategies to ensure that the appropriate data is sought to fully achieve the investigative objective.

7.67 In the operations where large elements of the offences, if not all the offences, took place within a 'virtual world' e.g. some of the fraud and sexual offences, the requirement for communications data was ever more apparent. It was also apparent from these operations that as technologies have developed police forces and law enforcement agencies have increasingly looked at a wider range of technologies to investigate offences. The inspectors noted that in relation to the investigation of serious and organised criminals, the increasing tactical awareness of criminals means that a larger amount of data, on a potentially wider range of devices and individuals, has to be acquired to meet operational objectives which may have been more simply achieved in previous years.

7.68 To summarise the inspectors found that a proportion of the communications data applications in each operation were not adequately formulated, i.e. they did not address the necessity or proportionality principles sufficiently. This does raise the question as to whether those represent significant institutional overuse. The inspectors also identified that in a couple of the operations examined there were potentially gaps in the acquisition process where the investigation teams had not identified the full range of data necessary to achieve the objective. I will come back to these points and try to answer the question after describing the other inquiries that we have undertaken in the reporting year, as a number of these have provided further evidence and assisted me to answer the question as to whether there is significant institutional overuse.

Inquiry into 999/112 emergency calls

7.69 The code of practice accompanying Chapter II of Part I RIPA 2000 acknowledges certain CSPs have obligations under the Communications Act 2003[37] relating to the provision of 999/112 emergency calls. Caller location information provides the geographical position of the equipment being used by the person making the emergency calls and facilitates a fast response where the caller to the emergency service is unable to give their location.

37 There are several EU Directives and Frameworks that contribute to make up the 999/112 Emergency Calls requirements – the Directive 2002/22/Ec Of The European Parliament And Of The Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). The Communications Act 2003 and the General Conditions of Entitlement transposes, into UK law, the various EU Directives and EU Frameworks relating to 999/112 Emergency Calls

7.70 Paragraph 4 of the General Conditions of Entitlement[38] published by Ofcom pursuant of the Communications Act 2003 (referred to as GC4) requires that where a Communications Provider provides an Electronic Communications Service:

(a) at a fixed location, the Caller Location Information must, at least, accurately reflect the fixed location of the End-User's terminal equipment including the full postal address (for example a landline's installation address); and

(b) using a Mobile Network, the Caller Location Information must include, at least, the Cell Identification of the cell from which the call is being made (for example the location of the mobile phone includes the mast and the cell through which the 999/112 call is made and the predicted coverage of the cell).

7.71 Systems[39] have been established that enable location information to be passed electronically to the emergency authority (police, ambulance, fire service etc.) at the time a phone call is connected from the emergency operator. However, on occasions the emergency authorities may require additional information to help locate the person making the 999/112 call, for example where the call is dropped or incomplete, or where the area covered by a cell-site may be large or unknown and the emergency authority may require more refined information to deploy an emergency service. The code of practice explains that emergency authorities may acquire 999/112 related data (as described in GC4) from emergency operators or the relevant CSPs for a period of up to one hour after the termination of the emergency call outside the provisions of RIPA 2000 in order to provide emergency assistance. In practice this communications data is acquired by staff within police force control rooms.

7.72 My inspectors undertook an inquiry to check that communications data was being acquired appropriately in these instances and, that the emergency provisions set by GC4 and the code of practice were not being abused. This inquiry was conducted between January and March 2014 and during that period 13 police forces were inspected. During these inspections the inspectors scrutinised the systems and procedures for acquiring communications data in relation to emergency calls within the forces' control rooms.

7.73 Our inquiry sought to establish how often police forces may receive calls where the caller location is not sufficient to deploy emergency services to the scene of the emergency and as a consequence, on how many occasions the police needed to acquire further communications data to assist in locating that caller. We also sought to determine whether the powers under RIPA 2000 had been appropriately invoked when police forces sought to acquire data within the emergency period that did not relate to the maker of the emergency call (for example, to investigate hoax 999/112 calls or, to respond to calls

38 See http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/generalconditions22nov12.pdf. Paragraph 4 of the General Conditions of Entitlement is often referred to in various publications relating to the provision of 999/112 Emergency Calls as GC4

39 See www.sinet.bt.com/sinet/SINs/pdf/278v2p1.pdf When an emergency 999/112 call is connected to the emergency service (for example the police) the BT Enhanced Information Services with Emergency Calls (EISEC) transmits the latitude / longitude of the building / mast upon which the cell plates are located, predicted cellular coverage plus the assurance level of the area indicated.

regarding a third party at risk).

7.74 **Subscriber information**. Without exception the police force control rooms sought subscriber information to assist in providing an emergency response and did so within the emergency period. The inspectors were satisfied that the data was acquired in appropriate circumstances and there was not an automatic recourse to acquire data. If the police could sufficiently identify a caller's location by other methods they would, and if the police thought that it was appropriate to call the person back to establish their location and whether they needed emergency assistance they would. Where the 999/112 system was being abused by hoax callers efforts to identify those responsible were dealt with using RIPA 2000 powers as would be the case with any other criminal matter.

7.75 **Traffic data (location information).** It was apparent from our inquiry that there was a varying capability in the different police forces to receive and comprehend the location information that was made available by CSPs to the emergency operators at the time a 999/112 call was connected. Furthermore, there were discrepancies as to what further location information (in addition to that relating to the original 999/112 call) that different CSPs were content to disclose to the police outside of the provisions of RIPA 2000 (when those incidents were still within the emergency period).

7.76 As mentioned above, systems have been established that enable location information to be passed electronically to the emergency authority (e.g. police) at the time a call is connected from the emergency operator[40]. Some forces have invested in technology which automatically maps the location information they receive electronically from the emergency operator; as a consequence, it was rarely the case that those forces needed to use their powers under RIPA 2000 to acquire location information. Other police forces did not have such technical systems, or, the staff in the control rooms lacked the skill to make use of the location information that was verbally relayed from the operator and these deficiencies could have led to delays in deploying an emergency service. To compensate for these deficiencies the control room staff called upon the services of an accredited SPoC to obtain data from the relevant CSP and in a number of these cases the urgent oral process under RIPA 2000 was invoked to acquire this additional location information. One police force reported that this accounted for 25% of all the SPoC's out of hours call out work while another reported that 14% of all the RIPA 2000 applications were undertaken to support 999/112 emergency calls.

7.77 Whilst in these circumstances the acquisition of data is appropriate, this still represents a technical 'overuse' of RIPA 2000 powers because this data should have been disclosed outside of RIPA 2000 as it was required within one hour of the termination of a 999/112 call to enable the provision of emergency assistance. In conclusion this inquiry has found some evidence of overuse of RIPA 2000 powers due to inadequacies in the 999/112 emergency provisions within some police forces.

40 See footnote 39

Inquiry into police force Professional Standards departments

7.78 Individual police forces have Professional Standards departments which are responsible for investigating complaints, misconduct, corruption and other unethical activity conducted by their own police officers and staff. In the reporting year my inspectors have focused on applications submitted by these departments to ensure that communications data has only been sought for the purpose of preventing or detecting crime and in cases where the investigating officer intends the matter to be subject of a prosecution within a criminal court[41]. The police cannot use their powers within RIPA 2000 to acquire communications data when the criminal threshold has not been met, or for the sole intention of obtaining evidence to merely to make an officer or member of their staff subject to an internal discipline hearing.

7.79 Where criminal conduct is suspected to have been undertaken by a police officer or member of staff and, where the intention is to make the matter subject of a prosecution within a criminal court, it may be necessary and proportionate for these departments to acquire communications data as part of the investigation. However should it be determined there are insufficient grounds to continue the criminal investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate for the police force to obtain communications data under RIPA 2000[42].

7.80 Misconduct in public office is a common law offence and can be widely applied. Guidance as to how this offence should be applied has been given by both the Crown Prosecution Service[43] and the Attorney General[44]. The former mentioned guidance includes basic advice to the effect that where there is clear evidence of one or more statutory offences, they should usually form the basis of the case, with the 'public office' element being put forward as an aggravating factor. The latter mentioned guidance outlines that the threshold of wrongdoing is a high one with four key elements:

- The suspect must be a public official acting as such;
- He or she must have wilfully breached his/her public duties;
- The breach must have been such a serious departure from acceptable standards as to constitute a criminal offence; and to such a degree as to amount to an abuse of the public's trust in the public official; and
- There must have been no reasonable excuse or justification.

7.81 The inquiry found that an excessively high number of the applications submitted by Professional Standards departments were completed to a poor standard and did not adequately justify the necessity and proportionality justifications. In a number of applications the criminal allegation or the criminal offences suspected were not set out or

41 See Footnote 14 of the Acquisition and Disclosure of Communications code of practice

42 See paragraph 2.2 and footnote 14 of the code of practice accompanying Chapter II of Part I RIPA

43 https://www.cps.gov.uk/legal/l_to_o/misconduct_in_public_office/

44 http://www.bailii.org/ew/cases/EWCA/Crim/2004/868.html

there was no description as to how they were linked to, and aggravated by, the officer's misuse of a position in public office. The applications often relied upon vague and dubious descriptions under the 'umbrella' of misconduct in public office and my inspectors were not satisfied that the high threshold for the offence of misconduct in public office had been met. There did not appear to be any intention for some of the matters to be subject of a prosecution within a criminal court. Turning to proportionality lengthy periods of traffic or service use data were often sought without sufficient justification and it was not clear whether other lines of inquiry had been considered and if so why they had not been pursued. For example, a number of the applications concerned investigations into officers forming inappropriate relationships with victims of crime. Whilst in some cases the circumstances may justify that it is reasonable to suspect serious inappropriate activity was taking place, for example, the formation of sexual relationships with vulnerable victims; some of the applications examined detailed fairly minor transgressions and did not identify whether serious wrongdoing was suspected, or failed to give convincing reasons to suspect that serious wrongdoing was occurring. In these applications it was also not apparent why other action, such as intervention by the officer's supervisors or misconduct interviews were not considered, or if they had been why they were not deemed appropriate. In such cases my inspectors concern was exacerbated where there appeared to be little resolve to subsequently pursue a prosecution when evidence was acquired which supported the initial premise of the application.

7.82 In conclusion this inquiry has identified that a number of the requests submitted by Professional Standards departments did not satisfy the necessity requirements and/or were disproportionate. As a result of these serious concerns my office engaged with the National Policing Lead for the Counter Corruption Advisory Group to outline the compliance issues identified. The National Policing Lead wrote to all police forces' professional standards leads and heads of department in December 2014 setting out our concerns and we expect to start to see improvements in compliance in this area. My office has also made recommendations for the SPoCs to exercise their guardian and gatekeeper functions more effectively in relation to applications submitted by Professional Standards departments.

Inquiry into the use of RIPA 2000 to acquire communications data to identify journalistic sources

7.83 In October 2014 due to the serious nature of the concerns reported in the media about the protection of journalistic sources, and the allegations that the police had misused their powers under Chapter II of Part I of RIPA to acquire communications data the Rt Hon. Sir Paul Kennedy, who was at the time acting as interim Commissioner, considered it necessary to launch an inquiry in this matter and make an additional report to the Prime Minister.

7.84 In February 2015 I published the report setting out the findings of my office's inquiry into these matters. This report[45] set out the extent to which these powers were

45 http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

used by police forces to identify journalistic sources, examined the appropriateness of this use, and made recommendations to ensure adequate safeguards are provided to protect journalistic sources.

7.85 In summary my office's inquiry found:

- In the 3 year period covered by the inquiry 19 police forces sought communications data in relation to 34 investigations into suspected illicit relationships between public officials (sources) and journalists.
- 608 applications were authorised to seek this communications data. This represented a very small percentage (0.1%) of the total applications that were authorised by the police in that period which demonstrated that such usage is not widespread. These figures were also artificially inflated by exceptional investigations like the Metropolitan Police's Operation Elveden – removing that investigation from the overall statistics provided context and would represent less than 1 application per police force per year (when averaged out over the 3 years and all UK police forces).
- Police forces had not circumvented other legislation by using their powers under Chapter II of Part I of RIPA 2000 to acquire communications data in these cases. However the observations of Emmerson and Friedman (1998)[46] appeared pertinent to the acquisition of communications data when reviewing its use to identify journalistic sources, i.e. that it undoubtedly has the potential to give rise to violations of Article 10 of ECHR[47].

7.86 All of the communications data applications had been authorised by a DP of the correct rank. The applications related to investigations where public officials were suspected of criminal conduct or where a media organisation had voluntarily disclosed information to the police.

7.87 Generally speaking the police forces did not give the question of necessity, proportionality and collateral intrusion sufficient consideration. They focused on privacy considerations (Article 8 of the ECHR) and did not give due consideration to freedom of speech (Article 10). Further information was required in the applications to justify why it was more important to identify the journalist's source than to respect their anonymity in the specific circumstances of the investigation. This included:

- a lack of specific detail about the information that had been (or was suspected to have been) leaked;
- whether in the circumstances of the case the high threshold for suspecting the common law offence of misconduct in public office had been met;
- insufficient consideration of whether the leaked information was of public interest merit;

46 Emmerson, B. QC., and Friedman, D. QC., A Guide to the Police Act 1997 (1998) Butterworths, (London) – p66 – 67

47 See paragraphs 6.25 to 6.29 http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

- what actual damage the leaked information had caused, or was likely to cause;
- whether the damage caused by the provision of that information amounted to a pressing social need justifying identification (and perhaps sanction) of the source;
- whether there was a disproportionately high risk of collateral intrusion into legitimate journalistic sources, and;
- a lack of detail about how the data would be analysed, processed and retained within the public authority to prevent unwarranted intrusion.

7.88 The current code of practice and the revised draft code of practice published in December 2014 do not provide any specific guidance on how DPs should actually apply the question of necessity, proportionality and collateral intrusion when dealing with data relating to sensitive professions, in particular journalists. The acquisition and subsequent analysis of data relating to communications with a journalist is likely to reveal journalistic sources and therefore general law relating to Article 10 of ECHR and the protection of journalistic privilege must be considered.

7.89 In light of these findings I made the following recommendations:

1 Judicial authorisation must be obtained in cases where communications data is sought to determine the source of journalistic information.

2 Where communications data is sought that does not relate to an investigation to determine the source of journalistic information (for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation) Chapter II of Part I of RIPA 2000 may be used so long as the DP gives adequate consideration to the necessity, proportionality, collateral intrusion, including the possible unintended consequence of the conduct. The revised code of practice contains very little guidance concerning what these considerations should be and that absence needs to be addressed.

7.90 I was pleased that the Government accepted my recommendations straight away and committed to implement the recommendations as soon as possible. I note that the Serious Crime Act, which received Royal Assent on 3rd March 2015 amended section 71 of RIPA 2000 to require the code of practice to include provision designed to protect the public interest in the confidentiality of journalist sources. In my view however the implementation of our recommendations required careful consideration and the interim measure is not ideal.

7.91 Coming back to my concern about whether there has been significant institutional overuse, the fact that a number of the applications that were examined as part of our journalist inquiry were not adequately formulated does raise the question as to whether those applications represent institutional overuse.

Conclusion regarding the inquiry into whether there is significant institutional overuse of Chapter II of Part I RIPA 2000 powers by police forces and law enforcement agencies

7.92 The various inquiries that my office has undertaken in the reporting year have resulted in a small number of instances being identified where the powers under RIPA 2000 should not have been used because:

(a) The data should have been acquired or disclosed outside the provisions of RIPA 2000 (i.e. using the 999/112 emergency provisions); or

(b) The requests did not meet the necessity criteria (for example in a small number of instances where data was acquired by Professional Standards departments the high threshold for the offence of Misconduct in Public Office had not been met and / or there was no intention for the matters to be subject of a prosecution within a criminal court; or

(c) The applications for communications data as formulated did not adequately set out the necessity or proportionality criteria.

7.93 The last category (c) does not mean however that given additional information the applications might not have been sustainable. In our operational reviews and a number of our additional inquiries we were able to interview relevant staff and obtain additional information and, in some instances on the basis of this we were satisfied that the requests were actually necessary and proportionate. However at scale we are generally only able to consider whether a particular application as formulated is necessary and proportionate.

7.94 To conclude, overall my office's inquiries did not find *significant institutional* overuse of communications data powers by police forces and law enforcement agencies. However, my office did find that a proportion of the applications did not adequately deal with the question of necessity or proportionality and we found some examples where the powers had been used improperly or where they had been used unnecessarily. Overall the operational reviews showed that the communications data that was acquired was necessary and proportionate to the matter under investigation.

7.95 My office intends to continue to conduct inquiries into specific issues to bring more meaning to how the powers are being used and to scrutinise the level of compliance being achieved by the public authorities. My office is in the process of examining the operational action and communications data strategies for certain types of offences (e.g. robbery) and is conducting a comparative study of investigations where communications data has and has not been acquired to ascertain the reasons why there might be differences and whether those differences might be indicative of an automatic resort to communications data where it may not be appropriate.

Communications Data Errors

7.96 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.

7.97 **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.

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

7.99 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;

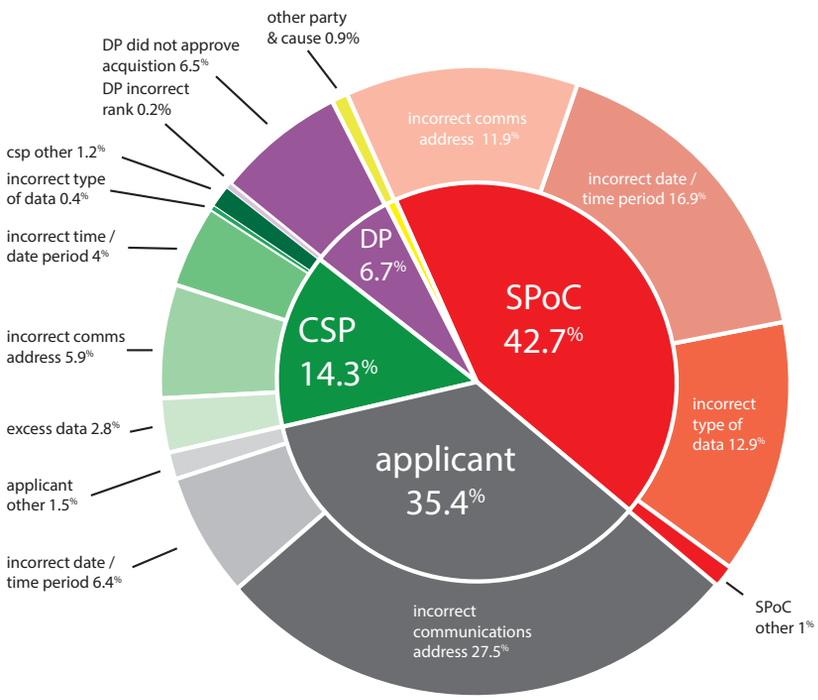
- explain how the error occurred,
- indicate whether any unintended collateral intrusion has taken place,
- provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur.

7.100 The total number of communications data errors reported to my office in 2014 was 998, which includes 13 found during inspections. This is slightly higher than last year's reported figure of 970 . The 998 errors should be seen in context of the 517,208 notices and authorisations.

7.101 In terms of how errors are counted, one erroneous act will typically correspond to one erroneous result (e.g. an applicant submits a request for subscriber data on the wrong telephone number and erroneous subscriber details are acquired). However on occasions one erroneous act, particularly where it relates to the programming of a system, may have multiple consequences and result in a larger number of erroneous disclosures.

7.102 In 2014 84.8% of the errors were attributable to public authorities, 14.3% to CSPs and 0.9% to other parties. Figure 13 shows the breakdown of errors by responsible party and cause. Errors mainly occur when public authorities erroneously seek, or CSPs wrongly disclose, communications data on the incorrect communications address (45.3%); or data for the incorrect time period (27.3%); or the wrong type of data (13.3%) on the correct communications address.

Figure 13 *2014 Breakdown of Errors by Cause*



7.103 Whilst it is inevitable that humans will make mistakes my office has continued this year to highlight where more can be done to reduce the number of human transposition errors. For example, we have made a number of recommendations for public authorities to implement measures to enable communications addresses to be copied and pasted between different computer systems to reduce the instance of transposition errors. My office reiterated the importance of this issue in a circular to all SROs in September 2014[48].

7.104 RIPA 2000 recognises that CSPs incur costs in complying with disclosure requests from public authorities and allows for arrangements for making appropriate payments to them to facilitate the timely disclosure of communications data. These arrangements are outlined in more detail in the Acquisition and Disclosure of Communications Data code of practice and may include funding to support bespoke disclosure systems, business overheads, staffing etc. Any CSP seeking to recover appropriate contributions towards its costs should make available to the Home Office such information or assurance as the Home Office requires to provide assurance that the proposed cost recovery charges represent an appropriate contribution towards the costs incurred by the CSP. Over recent years there has been a drive to update, maintain, or make more efficient CSPs disclosure processes and there are bespoke secure disclosure systems within some CSPs to manage the disclosures. These were introduced to reduce the amount of double keying and resultant human errors as well as to make more efficient CSPs disclosure processes.

48 http://www.iocco-uk.info/docs/ErrorsCirculartoSROs.pdf

7.105 It is crucial for such systems to be sufficiently tested prior to implementation and for quality assurance checks to be conducted regularly to ensure that any such systems are functioning effectively, particularly because one technical system error can have far wider consequences than one human error. Whenever such a system error is reported to my office an inspector is allocated to investigate the error instance thoroughly to determine the cause of the error, the extent of its impact and ensure that sufficient steps are taken to prevent recurrence. These investigations can take some time.

7.106 In the last reporting year I outlined that my office was in the process of investigating one such CSP system error which had resulted in incorrect data being disclosed to a large number of public authorities. This investigation is now complete and I can report that it was caused by a technical fault relating to the migration of subscriber records. The error resulted in the incorrect subscriber data being disclosed to a number of public authorities in relation to 361 data requests. Each one was followed up by my office and it was determined that in 5 cases individuals who were unconnected to the particular investigation being undertaken were visited by police. The individuals were all quickly eliminated from the police forces' inquiries and it was extremely fortunate that in the remaining 356 cases there was no significant impact as the police did not take any action on the incorrect disclosures. The incorrect data was destroyed in line with paragraph 6.21 of the code of practice as it had no relevance to the investigations being undertaken. This is an example of how one technical system error can have multiple and significant consequences.

7.107 In 2014 a further 12 technical errors were reported to my office (10 CSP and 2 police force / law enforcement agency). These 12 technical errors resulted in 1399 consequences. These have been, or are in the process of being investigated by my office. These investigations can take considerable time as each error has to be followed up with the public authorities affected by the disclosures to ascertain the significance of the consequences. In some of these cases the disclosure systems or parts thereof have been deactivated until the technical malfunction has been resolved. In addition to those significant technical errors, 9 human errors with very serious consequences were also reported to my office in 2014. Whilst every error is regrettable, the impact of most errors is limited in the sense that the error is quickly identified and the erroneous data destroyed, without any action being taken upon it. However, there are occasions where this is not the case and a public authority takes action against the wrong individual.

7.108 These 21 errors (12 technical and 9 human) resulted in action being taken against the wrong individual (for example, an innocent individual's address being visited by officers, or a warrant being executed at the wrong address) in 12 instances; and on 4 occasions caused a delay in the police conducting welfare checks on a person in crisis. Some of these errors occurred in relation to the resolution of Internet Protocol addresses and the consequences of these are particularly acute. An IP address is often the only line of enquiry in a child protection case, and it may be difficult for the police to corroborate the information before taking some form of action against the individual identified. Any police action taken erroneously in such cases, such as the search of an innocent individuals house, can have a devastating impact on the individual concerned. These errors are extremely regrettable and it is fortunate that errors with such severe consequences are

rare.

7.109 My next half-yearly report will concentrate on the 21 serious errors that were reported to my office in 2014 and provide full details in relation to the investigations that my office has undertaken. The report will outline the causes of the errors, the consequences and the measures that have been put in place to prevent recurrence.

Points of Note

Communications Data

In 2014 267,373 applications for communications data were authorised and these resulted in 517,236 authorisations and notices being issued or granted under Chapter II of Part I RIPA 2000.

172 public authorities acquired data in 2014. 88.9% of the applications for communications data were made by police forces and law enforcement agencies, 9.8% by the intelligence agencies and 1.3% by local authorities and other public authorities (regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions).

In 2014 my office conducted 90 communications data inspections. This is higher than l2013 because in 2014 my office moved to conduct annual inspections of the public authorities that acquire larger volumes of communications data. An additional 102 local authorities were inspected during the inspection of the National Anti Fraud Network (NAFN).

Our inspections are structured to ensure that key areas derived from Chapter II of Part I RIPA 2000 and the code of practice are scrutinised. Our inspectors have full access to the workflow systems used by public authorities and interrogate them. In 2014 my office scrutinised at random approximately 13,000 applications and in addition nearly 100,000 applications were subject to query based searches.

346 recommendations emanated from our inspections, on average 4 recommendations for each public authority.

Last year my office conducted a number of additional inquiries into specific issues. One of these inquiries looked into whether there is significant institutional overuse of communications data powers by police forces and law enforcement agencies. My office's inquiry concluded that there is not. But my office did find that a proportion of the applications did not adequately deal with the question of necessity or proportionality and we found some examples where the powers had been used improperly or where they had been used unnecessarily.

998 Chapter II of Part I RIPA 2000 communications data errors were reported to my office in 2014. 84.8% were attributable to public authorities, 14.3% to Communication Service Providers (CSPs) and 0.9% to other parties.

12 serious technical system errors were reported in 2014. Such errors can have multiple consequences and result in a large number of erroneous disclosures. In addition 9 human errors were also reported which had very serious consequences. These 21 errors resulted in action being taken against the wrong individual (for example, innocent individuals' addresses being visited by officers, or a warrant being executed at the wrong address) in 12 instances; and on 4 occasions caused a delay in the police conducting welfare checks on persons in crisis. My next half-yearly report will concentrate on these 21 serious errors and provide full details in relation to the investigations that my office has undertaken.

Section 8
Encryption

8.1 Part III of RIPA contains powers for public authorities to require disclosure of protected electronic information (electronic data) in an intelligible form or to acquire the means by which protected electronic information may be accessed or put in an intelligible form. The requirements of Part III are supplemented in detail by a code of practice *"Investigation of Protected Electronic Information"* 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)).

8.2 The measures in Part III are intended to ensure that the ability of public authorities to protect the public and the effectiveness of their other statutory powers are not undermined by the use of technologies to protect electronic information (such as passwords, encryption etc).

8.3 The National Technical Assistance Centre (NTAC), which provides technical support to public authorities, particularly law enforcement agencies and the intelligence services, includes a facility for the complex processing of lawfully obtained protected electronic information. NTAC is the lead national authority for Part III. No public authority may serve any notice under section 49 of RIPA 2000 or, when the authority considers it necessary, seek to obtain appropriate permission without the prior written approval of NTAC to do so.

8.4 There are three Commissioners with responsibilities under Part III: the Interception of Communications Commissioner; the Intelligence Services Commissioner; and the Chief Surveillance Commissioner.

8.5 My responsibilities under Part III are limited to keeping under review:

- the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under Part III, particularly the grant of appropriate permission for the giving of a section 49 notice in relation to information obtained under Part I (intercepted material and other related communications data); and
- the adequacy of the arrangements for complying with the safeguards in section 55 in relation to key material for protected information obtained under Part I.

8.6 Only persons holding office under the Crown, the police, a member of staff of the NCA or the HMRC may have the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by the Secretary of State.

8.7 It is the duty of any person who uses the powers conferred by Part III, or on whom duties are conferred, to comply with any request made by a Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions. The Commissioners' oversight also extends to NTAC.

8.8 I can confirm that no section 49 notices have been issued by the Secretary of State in relation to information obtained under Part I (intercepted material and other related communications data) since the start of my term in office (1st January 2013).

Section 9
Civil Monetary Complaints Function

9.1 The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interception) Regulations 2011 ("the Regulations") made amendments to Part I RIPA 2000 and provided additional protection for the users of electronic communications. In so doing, the Regulations addressed the concern expressed by the European Commission that the United Kingdom had failed to adequately transpose European Union (EU) law[49] requirements concerning the confidentiality of electronic communications, specifically in relation to the interception of communications.

9.2 RIPA 2000 regulates the lawful interception of communications for a range of legitimate purposes. It provides that interception can be lawfully undertaken either in accordance with a warrant signed by the Secretary of State or, in other specified circumstances[50], without a warrant. The changes to RIPA 2000, brought about by the Regulations, relate to interception without a warrant.

9.3 RIPA 2000 provides that communications service providers may lawfully and legitimately intercept communications when it is necessary for them to do so for specified purposes[51]. Where businesses choose to carry out interception to provide value-added services, an activity which is carried out at the discretion of service providers, RIPA 2000 requires the consent of both the sender and the recipient of the communications that will be intercepted[52]. It also provides for a criminal sanction against intended the interception of communications without lawful authority, thus providing additional protection for a person's privacy.

9.4 To address the deficiencies in the statutory regime that were identified by the European Commission, the Regulations amended RIPA in two respects. First, they created a civil sanction for the unlawful interception of electronic communications where the interception does not meet the standard of intent required in the criminal offence. Second, the Regulations clarified the nature of the consent that must be given by a party consenting to the interception of a communication to render that interception lawful. As a consequence, the words "reasonable grounds for believing" were removed from section 3 of RIPA 2000.

9.5 The Regulations introduce a monetary penalty that can be imposed, together with a requirement that the activity that has been determined to be unlawful under the regulations must stop. The sanction may be imposed by me if I am satisfied that certain communications have been intercepted without lawful authority at any place in the United Kingdom. In addition, I will need to satisfy myself that the actions are not already covered by the existing criminal offence of intercepting without lawful authority, and that the unlawful interception did not occur whilst attempting to act in accordance with an interception warrant.

9.6 The Regulations (and therefore the Interception Commissioner's responsibilities

49 In particular, the E-Privacy Directive and the Data Protection Directive

50 See sections 3(1), 3(2), 3(3) and 1(5)(c) of Part RIPA

51 See section 3(3) of RIPA

52 See section 3(1) of RIPA

under them) came into effect from 16 June 2011. My office has previously published guidance[53] in accordance with the Regulations. The guidance provides information on the circumstances in which I will consider it appropriate to issue a monetary penalty notice, how I will determine the amount of the penalty and the mechanism for handling complaints.

9.7 If a person has reasonable cause to believe their consent relating to their communications was not obtained during the provision of such a service they may seek to make a complaint to me under the Regulations. The complaints process is not the appropriate channel through which adverse comments about the way CSPs, based within the United Kingdom and elsewhere, conduct their business.

9.8 In 2014 my office received a number of complaints from members of the public, but we determined that all were in relation to conduct alleged to have been undertaken by public authorities. My office advised those individuals to make a complaint to the IPT who has exclusive jurisdiction in the United Kingdom to hear complaints of this type.

53 See http://iocco-uk.info/docs/Interception_Commissioner_Guidance_RIPA.pdf

Section 10
Telecommunications Act 1984

10.1 Section 94 of the Telecommunications Act 1984 covers directions in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

10.2 I have been asked recently by the Prime Minister to oversee directions issued under section 94 of the Telecommunications Act 1984. My oversight of section 94 will be on a non-statutory basis in the short term, but I hope that this can be addressed in the next Parliament.

10.3 I have confirmed with the Prime Minister that my oversight will include;

(a) Oversight of the necessity and proportionality of section 94 directions given by the Secretary of State;
(b) Oversight of the use of section 94 directions issued by the Secretary of State; and,
(c) Oversight of the safeguards for the use of section 94 directions.

10.4 My office is currently working at maximum capacity to discharge my statutory functions under RIPA 2000 effectively. I will therefore require extra staff (and possibly technical facilities) to be able to carry out this oversight properly. I do not anticipate that my requirements in this respect will be significant. However until I have determined the nature and full extent of the work being undertaken under any directions, and how the new oversight regime will be implemented, I will not be able to estimate exactly what resources will be required. Once I have done so, I fully expect to be provided with the necessary resources.

Section 11
Prisons

11.1 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.

11.2 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.

11.3 This non-statutory oversight of prisons in England and Wales commenced in 2002 at the request of the then Home Secretary. My office was invited to undertake inspections of the Northern Ireland Prisons by the then Director General of Northern Ireland Prisons in 2008.

11.4 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 49/2011, 56/2011, 24/2012, 10/2013, 07/2015, 10/2013) that impact on this area. Last year I made the point that the numerous policy documents are fragmented, overlapping 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. Since the previous reporting year our inspectors have again 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 again 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.

11.5 Last year I reported that NOMS was working towards implementing an Interception PSI. This has still not been implemented at the time of writing this report which is astonishing considering it has now been in draft for a number of years. I maintain the view that if an Interception PSI is introduced it should replace all other PSIs. Otherwise it will be very confusing for the establishments who are trying to introduce systems and procedures if there are numerous PSIs covering this activity and a lack of clarity over which PSI takes precedence.

11.6 Furthermore it is exasperating that NOMS has still not formally introduced the interception risk assessment template that was designed in 2011. My office has been informed that this is due to happen at some point in March 2015. Our inspectors have found themselves in a difficult position for several years now whereby they are effectively being asked to promote the use of templates which have not been formally ratified.

11.7 I reiterate that 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. Our inspections generally find that the prisons are trying extremely hard to comply with the various policies in this area, but they are in need of clear direction and better quality policy. The prison staff my inspectors meet during the inspections have

a willingness to carry out their work in this area to a good standard but recent cutbacks and benchmarking has led to an erosion of specialised roles and this work is now often undertaken by generalised staff who do not have the required experience and knowledge.

11.8 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. Last year I reported that this arrangement was far from ideal and I 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. To my knowledge this has not yet happened.

Authorisations to Intercept Prisoners' Communications

11.9 **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.

11.10 **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.

11.11 **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. 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. For example, 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.

11.12 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 Member of Parliament (MP).

11.13 On 11th November 2014 the Secretary of State for Justice, the Rt Hon. Chris Grayling launched an independent investigation after it was identified that a number of telephone calls between prisoners and their constituency MPs in England and Wales had been intercepted and some of those calls had been listened to. Her Majesty's Inspectorate of Prisons (HMIP) was asked to investigate the circumstances, to make recommendations to ensure that there were sufficient safeguards in place to minimise the risk of such calls being recorded inappropriately in the future and, to ensure that sufficient safeguards are in place for all confidential calls from prisoners. My office committed to fully support the investigation and we have done so. On 18th November 2014 my office met with HMIP to discuss the inquiry and provided their investigation team with a report outlining the number of recommendations that my office has made in relation to the handling of legal or otherwise confidential calls during our inspections of prisons. Although my inspectors had not identified any breaches with regard to calls to MPs, a significant number of recommendations had been made as a result of the inspectors identifying failures or areas for improvement with regard to the procedures for protecting or handling legal calls. It was noted that where such failings / issues had been identified, these recommendations would also read across to 'other' confidential calls.

11.14 The first stage of HMIP's inquiry was to undertake a review of the urgent, practical steps which NOMS were taking to minimise the risk of recording or listening to calls inappropriately in the future. A report[54] was published in relation to this stage of the inquiry on 28th November 2014. This report found that the urgent, interim measures taken by NOMS had been largely, but not wholly, effective in ensuring that prisoners' calls to MPs are not recorded or listened to. HMIP further reported that the technical measures that had been taken were effective but depend on the accuracy of the data that is inputted and so human error remained possible. The report outlined that it was necessary to resolve further technical queries and that more needed to be done to ensure that prisoners were aware of their responsibility to identify confidential numbers to prison staff. The second stage of the inquiry, which is looking at the circumstances around how the telephone calls came to be recorded in the past, has not yet reported. My office remains committed to providing HMIP with any assistance that they require to carry out their inquiry.

Inspection Regime

11.15 **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;

54 http://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2014/12/OFFICIAL-SENSITIVE-Prison-communications-report-for-publication.pdf

- 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.

11.16 Number of inspections. In 2014 our office conducted 100 inspections at 96 different prisons[55] which is over two thirds of the establishments.

11.17 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.

11.18 **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.

11.19 **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

11.20 The total number of recommendations made during our 100 prison inspections in 2014 was 492, an average of 5 recommendations for each prison. The marginal downward trend in the average number of recommendations emanating from each inspection has continued as exemplified by Figure 14.

11.21 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-

55 Four prisons were inspected twice in 2014 to ensure particularly poor levels of compliance were addressed promptly.

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.

Figure 14 *Total Red, Amber & Green Recommendations Resulting From Prison Inspections 2012-2014*

- Green recommendations - represent good practice or areas where the efficiency and effectiveness of the process could be improved.

11.22 This year 15.5% of the recommendations were red, 55.5% amber and 29% green.

11.23 Figure 15 shows the breakdown of the 2014 recommendations by category.

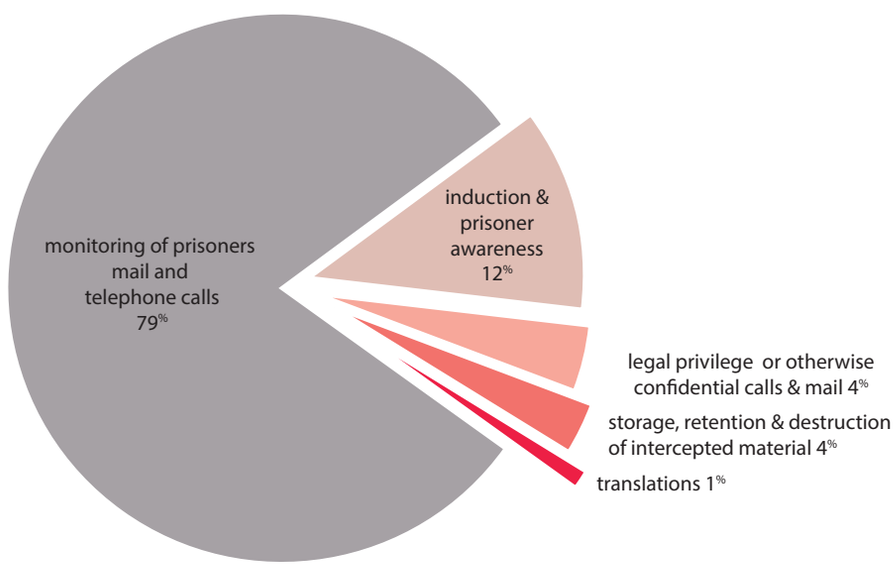
11.24 79% of the recommendations fell into 1 key category – procedures for the monitoring of prisoners telephone calls and mail. There are four distinct areas of failings in this category.

11.25 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 completed robustly or properly. In these instances the necessity and proportionality justifications for invoking or reviewing the monitoring had not been made out sufficiently. 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 prisoners' files and / or reviewed the minutes from risk management meetings where the prisoners had been discussed in an attempt to satisfy themselves that there was sufficient evidence to support the decisions.

11.26 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

Figure 15 *2014 Prison Inspection Recommendations by Category*



monitored in a timely fashion in order to evaluate properly the threat posed by prisoners.

11.27 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.

11.28 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.

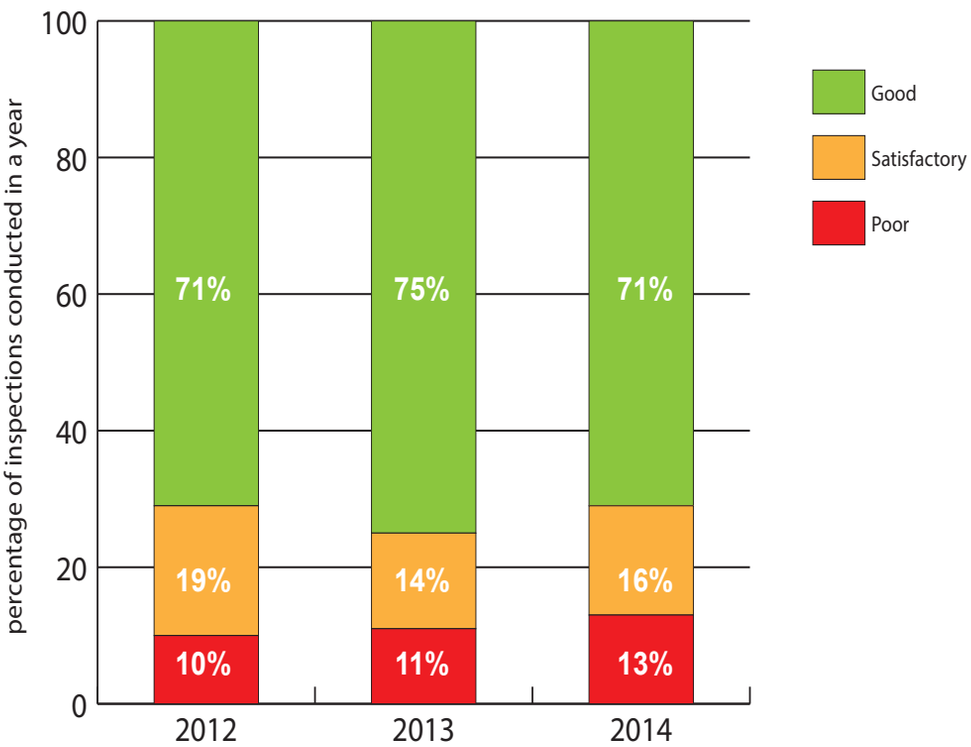
11.29 At the end of each inspection, each individual prison is given an overall rating (good, satisfactory, poor). This rating is reached by considering the total number of recommendations made, the severity of those recommendations, and whether those recommendations had to be carried forward because they were not achieved from the previous inspection. On the latter point, just over 80% of the prisons inspected in 2014 had fully achieved all or the majority of the recommendations emanating from their previous inspection.

11.30 Figure 16 shows that overall the proportion of prisons achieving a good level of compliance has remained fairly static in the last 3 years. However, it should be noted that comparisons with previous years are difficult because the prisons being inspected are not the same.

11.31 A more reliable way to gauge whether compliance is improving is to compare each prison's level of compliance from its 2014 inspection to its previous inspection rating:

- 64 inspections resulted in the level compliance remaining the same, with 56 prisons continuing to achieve a good level of compliance, 6 satisfactory and 2 poor.
- 16 inspections showed that there had been an improvement, with 8 prisons moving from a poor level of compliance to a good level, 7 from satisfactory to good, and 1 from poor to satisfactory.
- 20 inspections found that compliance had worsened, with 9 prisons moving from good to satisfactory, 8 from good to poor and 3 from satisfactory to poor.

Figure 16 *Overall Rating for Prison Inspections 2012-2014*



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.

In 2014 our office conducted 100 prison inspections. 492 recommendations emanated from these inspections, an average of 5 recommendations for each prison.

Last year I made the point that the numerous policy documents governing the interception of prisoners communications were fragmented, overlapping and contradictory in places and that this made it difficult for the prisons themselves to understand the requirements fully and for our inspectors to conduct the oversight. I am disappointed that there has not been any progress on these matters. I reiterate that NOMS must get to grips with these issues and put in place clear and defined policy and risk assessment documents for the interception of prisoners' communications. Our experience shows that the prisons are trying extremely hard to comply with the various policies in this area, but they are in need of clear direction and better quality policy.

79% of the recommendations fell into one key category – procedures for the monitoring of prisoners telephone calls and mail. The prison staff my inspectors meet during the inspections have a willingness to carry out their work to a good standard but recent cutbacks and benchmarking have led to an erosion of specialised roles and this work is now often undertaken by generalised staff who do not have the required experience and knowledge.

Just over 80% of the prisons inspected in 2014 had fully achieved all or the majority of the recommendations emanating from their previous inspection. The overall proportion of prisons achieving a good level of compliance has remained fairly static in the last 3 years. However, it should be noted that comparisons with previous years are difficult because the prisons being inspected are not the same.

Annex A: Public Authorities with access to Communications Data under Chapter II of Part I RIPA 2000

Public Authority Group	Data Type (RIPA s.21(4))			Statutory Purpose (RIPA s.22(2) & SI 2010/480) (as amended by SI 2011/2085, SI 2012/2007, SI 2013/472, SI 2013/602, SI 2014/549, SI 2015/228)										
	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	Art 2(c) regulation of financial services and markets	Notes
- Intelligence Services	•	•	•	•	•	•								
- Territorial Police Forces of England, Wales, Northern Ireland & Scotland - British Transport Police	•	•	•	•	•	•	•	•		•		•		(d) & (e) subscriber only
- National Crime Agency	•	•	•		•					•		•		(f) subscriber only
- The Commissioners for Her Majesty's Revenue and Customs	•	•	•		•				•					(d) subscriber only. Asylum fraud investigations can only acquire service use and subscriber information.
- The Home Office (Immigration Enforcement)	•	•	•		•		•					•		
- 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
- Gambling Commission - Gangmasters Licensing Authority - The Information Commissioner - Office of Communications - Police Ombudsman for Northern Ireland - Royal Mail Group - Serious Fraud Office	•	•	•		•									
- Financial Conduct Authority - Prudential Regulation Authority	•	•	•		•								•	Statutory purpose Art.2(c) was made available from 12/02/15

- Independent Police Complaints Commission - Police Investigations and Review Commissioner	•	•	•		•							•		
- 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 & subscriber 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 / Competition and Markets Authority - Pensions Regulator - NHS Protect - NHS Scotland Counter Fraud Services - The Department of Enterprise Trade and Investment (Northern Ireland)		•	•		•									
- Local Authorities		•	•		•									

Public authorities in yellow had their powers removed on 12/02/15 (SI 2015/228)

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

This Annex details the Total Applications approved, RIPA 2000 section 22(3) Authorisations granted or section 22(4) Notices given during 2014 by individual Public Authorities, excluding those given orally. It is organised according to public authority type*.

A total of 267,373 applications and 517,236 Notices and Authorisations (excluding urgent oral) were granted /given under Chapter II of Part I RIPA 2000 by 172 public authorities in 2014.

***Caveat:** The main report 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 Applications made, 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.*

It should also be noted that an Application for communications data may contain a request for one item of data or many items of data, and some public authorities require applicants to submit different applications for different types of communications data.

Because of the variability between applications and the inconsistent counting and aggregation of data requests on a single authorisation and notice the statistics, although accurately recorded by each individual public authority, are not necessarily comparable.

The Intelligence Services

	Total Applications	Total Notices & Authorisations
GCHQ	1,291	1,291
The Secret Intelligence Service (Mi6)	298	652
The Security Service (Mi5)	39,815	48,639
Grand Total	41,404	50,582

Police Forces & Law Enforcement Agencies

	Total Applications	Total Notices & Authorisations
Avon & Somerset Constabulary	5,510	8,766
Bedfordshire Police	1,864	2,468
British Transport Police	1,218	1,298
Cambridgeshire Constabulary	820	1,419
Cheshire Constabulary	2,064	4,247
City of London Police	1,049	2,174
Cleveland Police	1,336	5,591
Cumbria Constabulary	3,549	3,549
Derbyshire Constabulary	1,120	2,714
Devon & Cornwall Police	5,228	8,467
Dorset Police	710	1,879
Durham Constabulary	1,256	4,145
Dyfed Powys Police	1,149	1,474
Gloucestershire Constabulary	807	2,465
Greater Manchester Police	18,042	26,704
Gwent Police	1,568	5,588
Hampshire Constabulary	3,596	9,335
Hertfordshire Constabulary	4,708	8,723
Her Majesty's Revenue & Customs	6,219	10,397
Humberside Police	1,525	2,653
Kent Police & Essex Police	8,403	15,785
Lancashire Constabulary	4,203	11,471
Leicestershire Police	2,171	4,942
Lincolnshire Police	745	1,496
Merseyside Police	4,678	22,230

	Total Applications	Total Notices & Authorisations
Metropolitan Police	45,249	94,630
Ministry of Defence Police	29	141
National Crime Agency	24,665	41,716
Norfolk Constabulary & Suffolk Police	1,839	2,414
North Wales Police	1,228	2,342
North Yorkshire Police	1,017	1,538
Northamptonshire Police	1,473	3,194
Northumbria Police	2,663	5,979
Nottinghamshire Police	4,268	10,023
Police Scotland	11,778	24,303
Police Service of Northern Ireland	4,532	4,768
Royal Air Force Police	11	16
Royal Military Police	49	209
Royal Navy Police	1	11
South Wales Police	1,814	4,977
South Yorkshire Police	2,271	7,020
Staffordshire Police	2,310	5,162
Surrey Police	2,742	5,206
Sussex Police	1,725	5,340
Thames Valley Police	5,098	5,704
The Home Office (Immigration Enforcement)	561	4,602
Warwickshire Police & West Mercia Police	4,083	9,272
West Midlands Police	14,095	33,780
West Yorkshire Police	6,655	15,239
Wiltshire Police	1,317	2,353

Grand Total	225,011	459,919

The Civil Nuclear Constabulary, The Port of Dover Police and Port of Liverpool Police all reported that they did not grant any Authorisations or give any Notices in 2014

Some Police Forces share the services of a SPoC, and where this is so combined figures are reported.

Other Public Authorities

	Total Applications	Total Notices & Authorisations
Air Accident Investigation Branch	6	10
Criminal Cases Review Commission	2	2
Department for Business, Innovation & Skills	8	22
Department of Enterprise Trade & Investment (Northern Ireland)	28	167
Department for Environment, Food & Rural Affairs	2	3
Department of Work & Pensions - Child Maintenance Group	21	30
Environment Agency	22	22
Financial Conduct Authority	224	3,768
Gambling Commission	8	12
Gangmasters Licensing Authority	20	35
Health & Safety Executive	3	11
Independent Police Complaints Commission	13	30

	Total Applications	Total Notices & Authorisations
Information Commissioner's Office	28	35
Marine Accident Investigation Branch	1	1
Maritime and Coastguard Agency	3	3
Medicines and Healthcare Products Regulatory Agency	61	102
Ministry of Justice - National Offender Management Service	55	84
NHS Protect	4	10
Office of Communications	21	58
Office of Fair Trading / Competition and Markets Authority	2	2
Office of the Police Ombudsman for Northern Ireland	2	2
Rail Accident Investigation Branch	2	2
Royal Mail	71	164
Serious Fraud Office	32	50
Grand Total	639	4,625

The following 'other' public authorities reported that they did not approve any Applications, grant any Authorisations or give any Notices during 2014:

- Charity Commission
- Department of Environment Northern Ireland
- Department of Agriculture and Rural Development Northern Ireland
- Food Standards Agency
- NHS Scotland Counter Fraud Services
- Northern Ireland Office - Northern Ireland Prison Service
- Northern Ireland Health & Social Services Central Services Agency
- Pensions Regulator
- Prudential Regulation Authority
- Scottish Criminal Cases Review Commission
- Scottish Environmental Protection Agency
- No Fire Authority
- No Ambulance Service / Trust

Local Authorities

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

160 Local Authorities in England, Wales, Scotland and Northern Ireland reported they did not use their powers in 2014, but have used their powers in previous years

The following 95 Local Authorities reported using their powers in 2014:

	Total Applications	Total Notices & Authorisations
Aberdeenshire Council	1	1
Barnsley Metropolitan Borough Council	2	2
Bedford Borough Council	2	2
Birmingham City Council	12	23
Blackburn with Darwen Borough Council	2	11
Blackpool Borough Council	2	3
Bolton Metropolitan Council	2	6
Bracknell Forest Borough Council	1	2
Bridgend County Borough Council	2	4
Bristol City Council	3	3
Buckinghamshire County Council	5	30
Bury Metropolitan Borough Council	5	8
Caerphilly County Borough Council	2	6
Cambridgeshire County Council	4	5
Cardiff City and County Council	3	4
Ceredigion County Council	1	1
Cheshire East Council	3	7
Cheshire West & Chester Council	9	21
City of London Corporation	1	2
Cornwall County Council	2	14
Coventry City Council	7	32
Darlington Borough Council	4	5
Derbyshire County Council	1	1
Devon County Council & Somerset Council	5	9
Dudley Metropolitan Borough Council	2	6
Durham County Council	1	8
East Dunbartonshire Council	1	3
East Riding of Yorkshire Council	1	1
East Sussex County Council	1	11
Flintshire County Council	3	4
Gateshead Metropolitan Borough Council	5	8

	Total Applications	Total Notices & Authorisations
Glasgow City Council	1	7
Gloucestershire County Council	3	9
Hambleton District Council	1	4
Hampshire County Council	5	5
Hartlepool Borough Council	1	21
Hertfordshire County Council	2	15
Huntingdonshire District Council	2	2
Isle of Wight Council	1	4
Kent County Council	25	127
Kingston upon Hull City Council	1	1
Knowsley Metropolitan Borough Council	1	2
Lancashire County Council	12	46
Leicestershire County Council	5	11
Lincolnshire County Council	8	13
Liverpool City Council	8	23
London Borough of Barnet	2	33
London Borough of Brent	1	2
London Borough of Bromley	4	21
London Borough of Enfield	1	5
London Borough of Hammersmith and Fulham	1	19
London Borough of Havering	3	12
London Borough of Hillingdon	1	2
London Borough of Islington	3	7
London Borough of Newham	34	1,173
London Borough of Redbridge	3	28
London Borough of Wandsworth	1	2
Manchester City Council	1	4
Milton Keynes Council	2	16
Neath Port Talbot County Borough Council	2	7
Norfolk County Council	1	3
North Lanarkshire Council	2	3

Local Authorities continued...

	Total Applications	Total Notices & Authorisations
North Lincolnshire Council	7	10
Northamptonshire County Council	2	5
Northumberland County Council	2	6
Oldham Metropolitan Borough Council	5	11
Oxfordshire County Council	1	5
Perth and Kinross Council	2	13
Redcar & Cleveland BC	1	6
Rhondda Cynon Taff County BC	4	13
Rotherham Borough Council	3	3
Royal Borough of Greenwich	2	3
Royal Borough of Kensington and Chelsea	1	1
Salford City Council	1	2
Sheffield City Council	3	4
Slough Borough Council	1	2
South Gloucestershire Council	6	13
Southampton City Council	1	14

	Total Applications	Total Notices & Authorisations
St Helens Metropolitan Borough Council	8	16
Staffordshire County Council	2	2
Stirling Council	1	3
Stockport Metropolitan Borough Council	2	6
Stockton-on-Tees Borough Council	1	2
Stoke-on-Trent City Council	1	1
Suffolk County Council	1	3
Swansea City and County Council	5	20
Tameside Metropolitan Borough Council	1	3
Test Valley Borough Council	1	1
Thurrock Council	5	23
Torbay Borough Council	1	2
Warrington Council	4	19
Watford Borough	2	2
West Berkshire Council	3	14
West Lothian Council	2	4
York City Council	4	8
Grand Total	319	2,110

Annex C: Budget

My office's budget for 2014/15 was £1,066,800 allocated as below.

Expenditure for 2013/14 was not available at the time of print for the previous annual report, which was published on our website on 2nd June 2014 for ease we have included a copy for your information.

I am aware the salary, travel and subsistence costs will be less than the budget, due to the timing of recruiting of the recruitment of a new inspector and additional support staff.

2014/15 Budget

Description	Total (£)
Staff Costs	919,900
Travel & Subsistence	117,000
IT and Telecoms	5,600
Training & Recruitment	15,800
Office supplies, stationery, printing	6,000
Conferences & Meetings	7,300
Other	2,500

2013/2014 Expenditure

Description	Budget (£)	Actual Expenditure (£)
Staff Costs (13 Staff)	948,000	777,485
Travel & Subsistence	110,000	90,200
IT & telecoms	25,000	1,094
Recruitment, training and conferences	12,000	6,045
Office supplies, stationery, printing	3,500	5,529
Other	2,500	0
Total	**1,101,000**	**880,353**

ISBN 978-1-4741-1625-1