# Report of the Interception of Communications Commissioner

## Annual Report for 2015

(covering the period January to December 2015)

**The Rt Hon.**
**Sir Stanley Burnton**

# Report of the Interception of Communications Commissioner

## Annual Report for 2015
(covering the period January to December 2015)

**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 8 September 2016**

**Laid before the Scottish Parliament by the Scottish Ministers on 8 September 2016**

**HC 255**
**SG/2016/68**

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 9781474136396

Web ISBN 9781474136402

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

ID 12071602 07/16

Printed on paper containing 75% recycled fibre content minimum

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

The Rt Hon. Theresa May MP
Prime Minister
10 Downing Street
London
SW1A 2AA

18 July 2016

Dear Prime Minister,

I am required by section 58(4) of the Regulation of Investigatory Powers Act (RIPA) 2000, as amended by section 6 of the Data Retention and Investigatory Powers Act 2014, 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 year and, after the end of each half year.

My first report for this year was laid in Parliament earlier this month. That report covered IOCCO's review of directions issued under section 94 of the Telecommunications Act 1984.

I now enclose my second and final report for this year which covers the work which IOCCO conducted during the calendar year of 2015. Much of the work that this report covers was undertaken prior to my taking up office on 4 November 2015.

You are required to lay a copy of my half-yearly reports before each House of Parliament (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). My expectation is that you will feel able to lay this entire report before Parliament.

Yours sincerely,

The Rt Hon. Sir Stanley Burnton
Interception of Communications Commissioner

# Contents

# Section 1
# Introduction

**1.1** I was delighted to be appointed by the Prime Minister to undertake this important role at what is an especially significant and challenging time for investigatory powers. I took up my appointment on 4th November 2015 which coincided with the introduction of the Investigatory Powers Bill (IP Bill) into Parliament.

**1.2** This report covers the work the Interception of Communications Commissioner's Office (IOCCO) conducted during the calendar year of 2015. Much of the work that this report covers was undertaken prior to my taking up office. For this reason I have decided to retain the form and some of the legislative background and explanatory content from IOCCO's previous reports.

**1.3** I would like to acknowledge the work undertaken by my predecessor, the Rt Hon. Sir Anthony May to increase transparency and improve the public and Parliament's understanding of IOCCO's oversight regime and how the interception and communications data powers are used by public authorities. IOCCO have worked tirelessly to continue this important work, whilst carrying out its considerable inspection duties and investigations, and did so without a Commissioner for a significant period in 2015 owing to the failure of the Government to appoint a Commissioner when my predecessor stepped down in July 2015.

**1.4** 2015 was a significant and incredibly busy year for the matters which IOCCO is responsible for overseeing.

**1.5** Three independent reviews reported on the capabilities and powers required by law enforcement and the intelligence agencies, the regulatory and oversight frameworks and the privacy and security implications of the powers. IOCCO published written evidence[1] to David Anderson QC's review and gave oral evidence to the Intelligence and Security Committee (ISC) and the Royal United Services Institute (RUSI) reviews during which we shared our experiences, concerns, observations and findings.

**1.6** The reports[2] of these reviews were comprehensive and, as well as informing the public and political debate, they set out an extensive series of proposals for reform. After publication of the three independent reviews, the Government committed to bring forward a draft IP Bill by Autumn 2015 for scrutiny in Parliament by a Joint Committee of both Houses and stated that it would take into account the findings and recommendations of the reviews.

**1.7** In addition, a number of cases relating to the legislation that IOCCO oversees, were taken to the Investigatory Powers Tribunal (IPT). The IPT required assistance from

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

2 Privacy and Security Inquiry by the Intelligence and Security Committee (ISC) reported in March 2015 http://isc.independent.gov.uk/news-archive/12march2015. David Anderson QC's Investigatory Powers Review reported in June 2015 https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/. The Independent Surveillance Review by the Royal United Services Institute (RUSI) reported in July 2015 https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf .

IOCCO in connection with some of those cases as highlighted by the IPT in its recent report.[3]

**1.8** In 2015 new legislation was introduced relating to areas that are overseen by IOCCO and there were also a number of changes to the existing Codes of Practice for processes overseen by IOCCO. For example, public consultations concerning the Code of Practice for the Interception of Communications and the Code of Practice for the Acquisition and Disclosure of Communications Data led to revised Codes of Practice being issued.

**1.9** These not insignificant changes necessitated IOCCO altering its inspection regimes and, in some instances, providing guidance or further clarification to public authorities concerning the operational implications of the legislative and other changes.

**1.10** IOCCO continued to undertake its audits of public authorities' use of these intrusive powers under existing legislation and to make recommendations to improve compliance. In 2015 IOCCO carried out 172 inspections of public authorities and prisons and made 849 recommendations to improve compliance or to improve the systems and procedures for the interception of communications or the acquisition of communications data. Last year IOCCO reviewed over 1000 errors and conducted detailed investigations into those deemed to be serious. We are grateful for the assistance received from Communication Service Providers (CSPs) and public authorities with those investigations, and in particular the work that those bodies undertake to prevent recurrence.

**1.11** In February 2015 IOCCO published its inquiry report on the acquisition of communications data by police forces to identify or determine journalistic sources. The Prime Minister accepted the recommendations from that report immediately and the law was changed to provide more protection for journalistic sources.[4]

**1.12** IOCCO assisted Her Majesty's Inspectorate of Prisons (HMIP) to carry out its investigation into the interception of telephone calls between prisoners and their Members of Parliament (MPs).[5]

**1.13** In October 2015 IOCCO started its review of directions issued under section 94 of the Telecommunications Act 1984. Our review report was published on 7 July 2016.[6]

**1.14** Since my appointment I have reviewed a number of cases and exercised my

3 http://www.ipt-uk.com/docs/IPT_Report_2011_15.pdf

4 The Serious Crime Act which received Royal Assent on 3 March 2015 amended section 71 of RIPA to require the revised Code of Practice to include provision designed to protect the public interest in the confidentiality of journalistic sources. On 25 March 2015, the revised Acquisition and Disclosure of Communications Data Code of Practice came into effect requiring all law enforcement agencies to seek judicial authorisation when applying for communications data to identify or determine journalistic sources.

5 http://www.iocco-uk.info/docs/Prison%20communications%20report%20(print%20-%20correct).pdf

6 http://iocco-uk.info/docs/56208%20HC33%20WEB.pdf

powers under Paragraphs 6.22 and 8.3 of the Code of Practice for the Acquisition and Disclosure of Communications Data, to make determinations relating to serious errors or wilful or reckless conduct, and to inform affected individuals to enable them to consider whether to make a complaint to the IPT.

**1.15** Throughout this report we touch on these substantial matters in detail. At the end of each of the main sections of this report we have included "Points of Note" which summarise the contents of those sections. In **Annex D** we have included a glossary of terms and abbreviations.

**1.16** Overall I concur with the view of my predecessor that the inspections carried out by IOCCO show that the staff within the public authorities and prisons 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 errors occur. There is however always room for improvement. It is vital for IOCCO to continue to review the use of these intrusive powers with an independent eye to ensure that those who exercise the powers to protect the public in the interests of national security, to save life or to prevent or detect crime are doing so with sufficient consideration of the effect that the powers may have on fundamental rights and freedoms, such as the right to privacy and the right to freedom of expression.

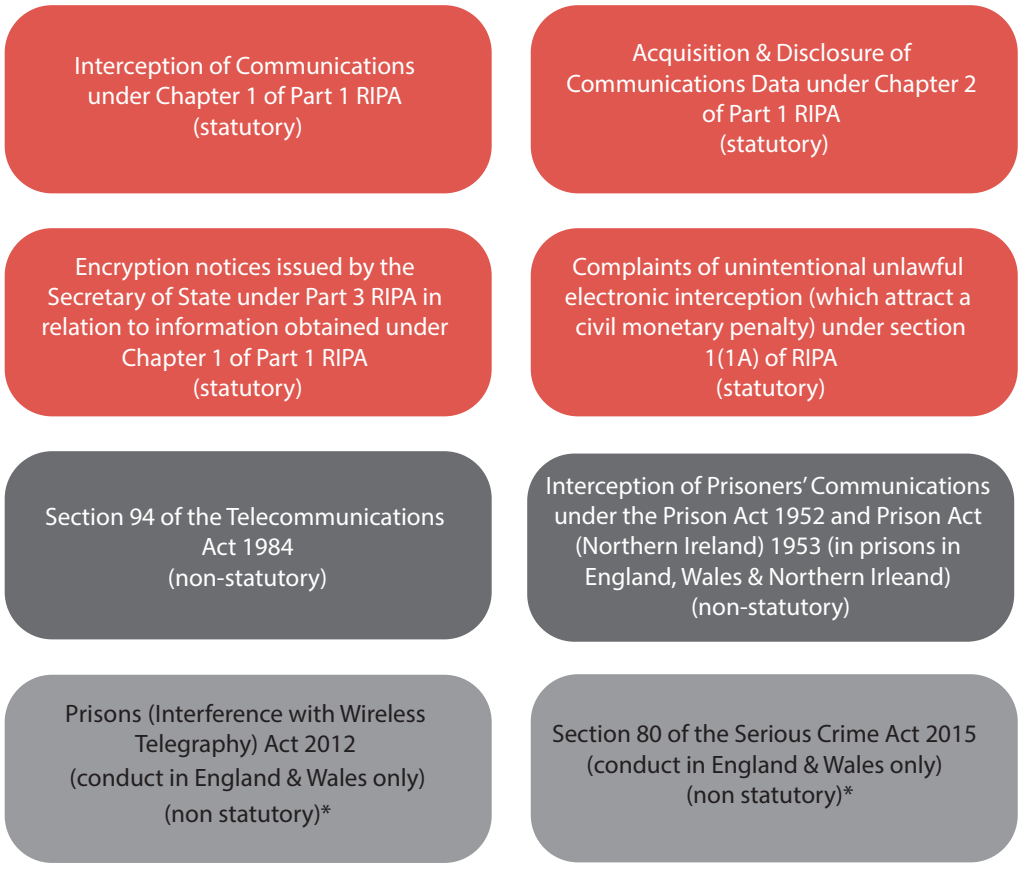
**1.17** There is significant public debate not only about the privacy implications of the public authorities' use of these intrusive powers, but also about the capabilities that the public authorities might require, the adequacy of the safeguards in the proposed legislation and, the effectiveness of the proposed oversight mechanisms. We shall continue to work with Parliament and the Government to ensure that the UK has legislation governing interception and communications data techniques that provides sufficient clarity, forseeability and transparency, which contains adequate human rights protections and safeguards, and which provides effective oversight and remedy mechanisms. IOCCO continues to contribute to the debates on, and scrutiny of, the IP Bill.

# Section 2
# IOCCO's Role

**2.1** IOCCO's principal duty is to assist the Commissioner to carry out his review of the exercise and performance, by the relevant secretaries of state and public authorities, of the powers under Part 1 (and to a limited extent Part 3) of the Regulation of Investigatory Powers Act (RIPA). IOCCO undertakes a number of other oversight functions, some of which are carried out on a non-statutory basis. **Figure 1** describes the functions of IOCCO.

**2.2** The Commissioner is independent of Government and Parliament and must report half-yearly[7] to the Prime Minister on the carrying out of his functions. Independent oversight plays a key role in contributing to accountability. The purpose of oversight is to ensure that there are strong checks and balances, demanding and visible safeguards, and that public authorities are held to account. It is to check that action undertaken

**Figure 1** *IOCCO's oversight functions*




*We have recently been asked by the Home Office & Ministry of Justice to undertake this additional oversight on a non-statutory basis. We have agreed, subject to receiving a formal direction from the Prime Minister and some additional resources.

7 The half-yearly requirement was introduced under the Data Retention and Investigatory Powers Act (DRIPA) 2014 and therefore expires with the DRIPA sunset clause on 31 December 2016. From 1 January 2017 IOCCO will revert to annual reports to the Prime Minister, unless new legislation is in force and provides otherwise.

is necessary and proportionate, and to ensure that when errors occur individuals can exercise their right to an effective remedy.

**2.3** As well as contributing significantly to accountability, oversight also aids transparency. For the last few years IOCCO have striven to improve transparency and inform the public better about what the legislation allows, how IOCCO carries out its oversight, the use public authorities make of these intrusive powers and the level of compliance that the public authorities and prisons are achieving. We have a website and a Twitter account on which we publish frequent guidance documents, statistical information, recommendations, speeches, press statements, inquiry reports etc. Since 2013 our reports to the Prime Minister have been published in full with no confidential annex.

**2.4** Our function, as debated and decided by Parliament, is to *"conduct audits and to check what is happening in practice, rather than to examine every case universally."*[8] We have introduced a vigorous inspection regime to enable us to carry out our function effectively. Section 58(1) of RIPA imposes a statutory obligation on everyone concerned with the powers we oversee to disclose or provide to the Commissioner all such documents or information as may be required for the purpose of enabling him to carry out his functions under section 57 of RIPA.

**2.5** IOCCO is not a promoter of the legislation or of the public authorities' use of it. Our 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 to decide upon. The IPT has an exclusive role in the UK in proceedings for actions that are incompatible with the European Convention on Human Rights (ECHR).

**2.6** Under Section 57(7) of RIPA, the secretary of state is obliged to consult with the Commissioner and to make such technical facilities available and, subject to Treasury approval as to numbers, to provide the Commissioner with such staff as are sufficient to ensure that he is able properly to carry out his functions. The Commissioner is supported in his role by the Head of IOCCO Joanna Cavan, a team of ten inspectors and two secretariat. IOCCO's staff are independent, highly skilled and experienced in the principles and detail of RIPA. The inspectors have been recruited from a wide variety of backgrounds and bring with them a broad range of experience. Their expertise covers the fields of legal, policy, investigative, analytical and forensic telecommunications. They have extensive experience of working with police forces, intelligence and law enforcement agencies, industry regulators, universities and telecommunications-related private organisations, and some have acted as accredited Single Points of Contact (SPoCs), Senior Responsible Officers (SROs) and Designated Persons (DPs).

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

# Section 3
# Transparency and Accountability

**3.1** There continues to be significant public debate about the privacy implications of public authorities' use of investigatory powers, the capabilities the public authorities have and might require, the adequacy of the existing legislation and the effectiveness of the oversight mechanisms.

**3.2** We continue to provide the public and Parliament with information about what we do. Our aim is to improve transparency around how interception and communications data powers are used by public authorities, the level of compliance being achieved by those authorities and the safeguards in place. We believe this demonstrates our commitment to understanding the key issues and informing the public about what we do.

**3.3** **Website and Twitter.** In 2015 we included more information on our website to make our published reports more accessible and ensure that our press statements, speeches, guidance documents, inquiry reports and various evidence papers are available to the public. Throughout the year we have published various documents on our website (www.iocco-uk.info), issued press statements about matters under investigation and published the findings of our inquiries. Our Twitter account (@iocco_oversight) has allowed 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 field of work. It helps us to keep up to date with relevant news and is a valuable tool for following discussions and gleaning new information from academics, researchers, lawyers, civil society, think tanks, computer scientists and key individuals working in our field. Both our website and Twitter account are important media, enabling us to communicate and report promptly with greater flexibility than we could otherwise achieve through our reports before Parliament.

**3.4** **Enhanced statistical requirements.** We have for some time called for enhanced and accurate statistical requirements to help clarify the volumes and types of communications data acquired by public authorities. We were pleased that the Home Office implemented our recommendations and amended the statistical requirements in the revised Code of Practice accompanying Chapter 2 of Part 1 of RIPA. **Section 7** of this report sets out a number of the new statistics which have improved transparency and accountability. We continue to push for similar statistical requirements for interception under Chapter 1 of Part 1 of RIPA.

**3.5** **Public speaking.** In 2015 we were delighted to accept invitations to speak publicly about our role and work at numerous events including;

- Wilton Park: Privacy, public safety and policing in the digital age: a UK perspective event;
- The Computers, Privacy and Data Protection Conference in Brussels;
- The Oxford Intelligence Group - Snowden, the Media and the State event;
- The Scottish Public Law Group Surveillance event;
- The International Communications Data and Digital Forensics (ICDDF) conference;

- The iCLIC conference at Southampton University: Enrolling Internet Intermediaries in the Law Enforcement Process Challenges & Opportunities;
- The Internet Service Providers Association (ISPA) 20th Anniversary Conference - "The Future Communications Landscape";
- JUSTICE and King's College London round table "A surveillance Framework for a Digital Age: Authorisation, Oversight and the Judiciary".

**3.6** We also attended a number of other relevant events through the year including those run by the Parliamentary Internet, Communications and Technology Forum (Pictfor), the Parliament & Internet Conference and the Cityforum Cyber Security Masterclass & Round Table with the National Security Agency.

**3.7** **Assistance to the reviews.** We provided assistance to the three independent reviews in 2015 – the Privacy and Security Inquiry by the ISC, David Anderson QC's Investigatory Powers Review and the Independent Surveillance Review by RUSI. We met with David Anderson QC to discuss our written evidence[9] and gave oral evidence to the ISC and RUSI, sharing our experiences, concerns, observations and findings.

**3.8** **Parliamentary committees.** We were pleased to be invited to give oral evidence to the IP Bill Joint Committee of Parliament in December 2015. We provided written evidence to the Committee which highlighted, among other things, a number of concerns and inadequacies with the clauses in the IP Bill and made suggestions as to how the oversight arrangements might be strengthened.[10] We have already provided updates to that evidence and will continue to do so.

**3.9** **Assistance to the Home Office.** We met regularly with the Home Office policy team and the communications capability directorate to discuss the various legislative consultations, policy matters and projects being undertaken. During these meetings we provided independent advice on how to strengthen the safeguards, improve compliance and increase transparency.

**3.10** **National Police Chiefs' Council (NPCC) Data Communications Group (DCG) tradecraft events.** We attended a number of learning events for Single Points of Contact (SPoCs), Senior Investigating Officers (SIOs), Designated Persons (DPs), investigating officers and analysts. This included a workshop on protecting journalistic sources and a distance learning event on the independence of DPs. We also ran workshops at the ICDDF conference on errors, frequent recommendations resulting from our inspections and the legislative landscape.

9 http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

10 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20IP%20Bill%20Joint%20Committee.pdf

**3.11** **Senior Responsible Officer (SRO) circulars.** We have published a number of circulars to SROs to help them prepare for IOCCO inspections and to review compliance regularly within their own public authority. A number of the circulars provide further guidance to help SROs comply with the revised statistical requirements and to interpret certain provisions in the Acquisition and Disclosure of Communications Data Code of Practice (March 2015), for example those relating to the independence of DPs. We have recently published new communications data error report form templates to ensure that errors are reported to IOCCO comprehensively. All of these circulars can be found on our website.

**3.12** **Membership of panels / boards.** At the invitation of the NPCC we joined the Professional Oversight Board, a standing committee that reports to the NPCC DCG Executive Committee, which is responsible for developing, monitoring and promoting excellence in lifelong learning processes, strategies and tools for professional practice for communications data.

**3.13** Joanna Cavan, Head of IOCCO is also a member of the newly formed Independent Digital Ethics Panel for Policing, a formal mechanism by which the NPCC and the National Crime Agency (NCA) can test ethical boundaries for policing an increasingly complex and digitised Britain. The panel is independent of the NPCC and Government, and it provides insight and challenge in relation to a range of areas associated with digital policing and cyber crime.

**3.14** **Communication Service Provider (CSP) engagement.** IOCCO have a strategic relationship with the CSPs, which assists us greatly in carrying out our oversight functions. We attend regular meetings with CSPs to keep abreast of technology, data retention and disclosure mechanisms, to discuss legislation and policy and to investigate errors.

**3.15** **Non-governmental organisations (NGOs), academics, lawyers and other key experts.** The work we undertake is enriched by and benefits from our engagement with academics, technical experts and privacy advocates. We continue to meet regularly and engage with colleagues from think tanks and civil society organisations to discuss relevant issues and concerns. We are grateful to these individuals, in particular to the NGOs, for continuing to challenge us on areas of our work such as transparency. We will continue to engage with and seek advice from such individuals.

**3.16** **International relationships.** We have hosted or visited a number of our international counterparts to discuss our respective oversight regimes, inquiries and investigations and to share our experiences. Last year we met with our counterparts from the following bodies:

- the Dutch Review Committee on the Intelligence and Security Services (CTIVD);
- the Australian Parliamentary Joint Committee on Intelligence & Security;
- Susie Alegre, the Interception of Communications Commissioner for the Isle of Man;

- Cheryl Gwyn, the New Zealand Inspector-General of Intelligence and Security;
- Alexander Joel, Chief, United States Office of Civil Liberties, Privacy and Transparency (CLPT).

**3.17** We have plans in 2016 to meet with a number of our other international counterparts.

# Section 4

## The Data Retention and Investigatory Powers Act (DRIPA)

**4.1** DRIPA[11] received Royal Assent on 17 July 2014. IOCCO published its full response[12] to DRIPA shortly thereafter. To meet the requirements expressed by Parliament during the passing of the bill, IOCCO was asked to report on whether DRIPA, in practice, does exactly what the Government said it would[13] and to reassure Parliament that DRIPA is implemented in the way Parliament intended.[14]

**4.2** We provided updates on the implementation of DRIPA in our March 2015[15] and July 2015[16] reports and do not intend to repeat those extracts, apart from our broad conclusions which are unchanged. The amendments to the various definitions and explicit assertion of extra-territoriality in DRIPA do not appear in practice to have resulted in an extension of powers and do not appear to have changed or amended the operational practice of those public authorities using their powers under Part 1, or the conduct undertaken by overseas CSPs.

**4.3** Whilst overseas CSPs receive notices under section 22(4) of RIPA requiring the disclosure of communications data, the CSPs continue to maintain that the notices cannot be enforced or compelled through civil sanction within the UK as they are 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 CSP's view they are disclosing the data "voluntarily" and are not compelled to do so.

**4.4** With regard to interception warrants, although the number of overseas CSPs co-operating has improved, they continue to provide voluntary assistance in limited circumstances. The Government has not, so far, taken steps to enforce the duty under section 11 (as amended by DRIPA) to comply with an interception warrant.

**4.5** On 15 July 2016 the United States (US) Government presented a legislative proposal for the consideration of Congress that would help resolve potential conflicting legal obligations that US electronic CSPs may face when required to disclose electronic data by foreign Governments investigating serious crime, including terrorism.[17]

---

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

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

13 Home Secretary comments in Hansard Column 708 *".....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....."*

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

15 See section 5 http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

16 See section 2 http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf

17 https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4

# Section 5
# Investigatory Powers Bill

**5.1** We mentioned earlier in this report that in 2015 three independent reviews reported on the capabilities and investigatory powers required by law enforcement and the intelligence agencies, the regulatory and oversight frameworks and the privacy and security implications of the powers.

**5.2** We have carried out a significant amount of work and published a number of documents to assist the various reviews, committees, parliamentarians and other key stakeholders. Our aim has been to help them to understand the safeguards to protect privacy, the case for amending or replacing legislation, the statistical and transparency requirements that should apply to the powers, and how the oversight provisions can be developed and strengthened to improve the effectiveness of the current oversight arrangements.

**5.3** This section describes that work in chronological order and provides links to our numerous publications. We would encourage the reader to review our publications to track the status of the various suggestions for enhancements or recommendations that we have made.

**5.4** We published written evidence[18] to David Anderson QC's review and gave oral evidence to the ISC and RUSI reviews during which we shared our experiences, concerns, observations and findings. The reports[19] of the three independent reviews were comprehensive and, as well as informing the public and political debate, they set out an extensive series of proposals for reform.

**5.5** The review reports addressed a number of the concerns and inadequacies that we highlighted with regard to the current legislative framework and the safeguards to protect privacy. David Anderson QC in his "A Question of Trust" report recognised the significant efforts that we have made to improve transparency and accountability through our reports to Parliament, additional inquiries, investigations and publications, various public engagements and social media presence. David Anderson QC said that "*having spoken in depth to IOCCO, and reviewed a number of reports of similar review bodies from different countries, I would comment that they are a model of their kind*". RUSI commented that "*the offices of some of the commissioners are very proficient (especially IOCCO).*"

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

19 Privacy and Security Inquiry by the Intelligence and Security Committee (ISC) reported in March 2015 http://isc.independent.gov.uk/news-archive/12march2015. David Anderson QC's Investigatory Powers Review reported in June 2015 https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/. The Independent Surveillance Review by the Royal United Services Institute (RUSI) reported in July 2015 https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf .

**5.6** On 3 November 2015 we published our "wish list"[20] of the six elements we would like to see in the IP Bill to strengthen the current oversight of surveillance powers:

1. **A single independent public facing oversight body.** We support fully a single unified body with responsibility for surveillance oversight. This will be an opportunity to streamline the oversight landscape, to put all of the oversight responsibilities on a statutory footing, to bridge some of the identified gaps and remove overlaps. The body must be independent, have an appropriate legal mandate and be public facing to promote greater public trust and confidence.
2. **Full access to technical systems.** RIPA contains outdated language (a requirement to provide to the Commissioner with "all such documents and information") and is in need of updating. The query based examinations we have developed enable us at scale to identify trends, patterns and compliance issues across large volumes of applications. We need to develop our technical audits on the interception side of the business, particularly where the collection of material and data is at scale and in order to do so we need explicit provision to access systems.
3. **Provision to launch investigations and sufficient resource to conduct thematic inquires.** The oversight body should have a clear mandate to launch inquiries into matters of public interest or areas of concern. Detailed thematic investigations should take place in addition to ongoing reviews. It is difficult presently for us to produce detailed thematic reports without undermining our core review functions - both are key to ensuring robust oversight and one should not compromise the other.
4. **Relaxation on secrecy provisions to aid transparency.** We are constrained by the current statutory provisions in section 19 of RIPA forbidding disclosure, as are the public authorities and the CSPs. The culture of secrecy must continue to be challenged and transparency should be encouraged where it leads to greater accountability without prejudicing national security or the ongoing prevention or detection of crime.
5. **Full provision for reporting errors / breaches and power to refer matters to the IPT.** It is crucial to ensure that the error reporting provisions are clear and comprehensible and that individuals adversely affected are able to seek effective remedy. On the latter point a number of areas would benefit from review here including; the threshold of "wilful or reckless" and whether the Commissioner should be able to refer matters directly to the IPT.
6. **Expert resource to complement the Commissioner.** To complement the Commissioner's expertise a breadth of skills are required, for example, staff with technical skills (such as computer scientists, engineers), analytical expertise, investigative experience, privacy and public interest advocates, media and communications expertise. A broad and in-depth range of skills will ensure that the public authorities are robustly held to account and that all critical views are represented.

20 http://www.iocco-uk.info/docs/Kings%20College%20Round%20Table.pdf

**5.7** On 4 November 2015 the Government introduced the IP Bill into Parliament and it has since gone through various iterations.

**5.8** The bill was scrutinised by a Joint Committee of both houses, the House of Commons Science and Technology Committee and the ISC, resulting in over 150 recommendations.[21]

**5.9** We submitted written evidence[22] and gave oral evidence[23] to the Joint Committee highlighting the elements needed to create a world-leading oversight body, along with a number of additional concerns and inadequacies relating to the IP Bill clauses. We summarised our evidence into eight key areas and were pleased that the Joint Committee and the ISC made over 20 recommendations in the areas we highlighted. On 25 February 2016 we published a one page summary linking the various Committees' recommendations to our evidence.[24]

**5.10** On 1 March 2016 the Government introduced the revised Bill to Parliament and published a substantial amount of additional documentation to accompany the Bill. One of these, the *Government's Response to Pre-legislative Scrutiny,*[25] included a table of the various Committees' recommendations and the Government's response to each.

**5.11** On 23 March 2016 we published[26] a document that sought to review the 8 key areas we had highlighted in our original written evidence to the Joint Committee against the revised IP Bill that was introduced to Parliament on 1 March 2016. We did so in order to assist the Public Bill Committee which was at that time carrying out a detailed line by line examination of the Bill. We also gave oral evidence[27] to the Public Bill Committee.

**5.12** **Update at House of Lords stage:** At the point at which this report was finished, the IP Bill had progressed to the House of Lords. The comments in the following paragraphs relate to the iteration of the IP Bill that was introduced into the House of Lords on 8 June 2016. Although it contained some enhanced safeguards we still have concerns that a

21 Joint Committee report http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm ; Science and Technology Committee report http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf ; ISC report http://isc.independent.gov.uk/committee-reports/special-reports

22 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20IP%20Bill%20Joint%20Committee.pdf

23 http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf

24 http://www.iocco-uk.info/docs/Summary%20of%20Points%20to%20Consider%20on%20IP%20Bill%20and%20recommendations.pdf

25 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF

26 http://www.iocco-uk.info/docs/Points%20to%20Consider%20on%20IP%20Bill%20and%20recommendations%20-%20updated%20post%201st%20March%20amended%20Bill.pdf

27 http://www.publications.parliament.uk/pa/cm201516/cmpublic/policingandcrime/160324/pm/160324s01.pdf

number of the elements on our original "wish-list" are not explicitly provided for. This is a missed opportunity to enhance safeguards and strengthen further the oversight provisions. Our concerns are as follows:

**5.13** We are disappointed that the Government has still not created or made any reference to an oversight Commission in the IP Bill, despite repeatedly giving a commitment to creating "world leading oversight". The oversight provisions in the IP Bill need to prescribe properly the legal mandate of the "Commission" in order to set the standard for a modern, independent oversight body.

**5.14** At present clause 203 of the IP Bill only creates a Chief Judicial Commissioner and a small number of Judicial Commissioners. The commissioners will only be responsible for approving approximately 2% of the applications falling within the remit of the oversight body. The remaining 98% will only be subject to post-facto oversight. The post-facto oversight will be carried out predominantly by specialist inspectors, investigators, analysts and technical staff within the Commission and it is important for those individuals to have a delegated power to require information or access to technical systems. The creation of a Commission is crucial to achieve a modern, inquisitive oversight body that has the expertise to carry out investigations and inquiries to the breadth and depth required and the intellectual curiosity to probe and challenge the conduct of the public authorities. Putting the oversight Commission on a statutory footing will be a huge step towards guaranteeing independence, capability and diversity within the organisation which will inspire public trust and confidence.

**5.15** Creating an oversight Commission would also help make a distinction between the approval and post-facto audit elements of the oversight body, addressing a concern raised by a number of witnesses to the Joint Committee that the Judicial Commissioners should not be perceived to be "marking their own homework".

**5.16** We urge the Government to implement this recommendation which was also made by the RUSI Independent Surveillance Review, David Anderson QC and the IP Bill Joint Committee.

**5.17** The secretary of state remains responsible for providing the Commissioner with the funding, staff and facilities that *the secretary of state considers necessary* for the carrying out of the Commissioners' functions (clause 213(2) of the IP Bill), despite the Joint Committee suggesting rightly that it was inappropriate for the secretary of state alone to determine the budget of the body which is responsible for reviewing the secretary of state's performance.

**5.18** Clause 207 makes provision for the Investigatory Powers Commissioner to inform individuals of any serious errors, but an error cannot be deemed to be serious unless it has caused significant prejudice or harm to the person concerned. We still have a number of concerns with this clause. First, the description of a "serious error" appears to be dependent on the consequence of the conduct, rather than on an assessment of the seriousness of the conduct itself. Later in this report we provide guidance in relation to the types of errors we currently consider to be "serious" which is not purely based

on the consequence of the conduct. Secondly, there is still no complete definition of "relevant error" in clause 207(9) which appears to still be confined to public authority conduct, even though around 21% of interception errors and 13% of communications data errors are caused by CSPs. The draft IP Bill Codes of Practice should provide clarity and further detail on these points but at present they do not. Thirdly, we have concerns that the threshold is set artificially high, which will prevent individuals from being able to seek effective remedy. We note that the Government has committed to review the threshold for error reporting (see the Government response to IP Bill Joint Committee recommendation 58[28]), but we have not seen any evidence of this review as yet.

**5.19** The Joint Committee's recommendation to remove the national security exemption relating to the requirement for DPs to be independent of investigations or operations when approving communications data has *not* been implemented. Clause 59 still includes a broad exemption for national security purposes which dilutes considerably the strengthened process introduced in the March 2015 Acquisition and Disclosure of Communications Data Code of Practice which came about as a result of the Digital Rights Ireland Judgement by the European Court of Justice (ECJ). The Government's response sets out that the exemption only applies in "exceptional and particular cases" and that it is not a blanket exemption. However, in our view that position is not reflected in the drafting of clause 59.

**5.20** Clause 72 has not been amended and still disapplies the requirement for a public authority to consult with a SPoC when acquiring communications data *in the interests of national security*. The SPoC is a key safeguard in the process and the justification for considering the interests of national security always to be an exceptional circumstance is unclear.

**5.21** The Government has not taken the opportunity to bring all of the investigatory powers used by public authorities into the IP Bill (e.g. Part 2 of RIPA which covers directed and intrusive surveillance authorisations for law enforcement) and curiously it prescribes different authorisation and modification procedures for targeted equipment interference warrants made on behalf of the intelligence services to those on behalf of law enforcement. The different application and approval procedures are confusing, lack clarity, and it is not clear on what basis they are justified. We agree with others that this is a missed opportunity.

**5.22** In our 2015 report the former Commissioner made clear that it would be preferable if our prison oversight was formalised as a statutory function. Our understanding is that the Government intended to do this in the IP Bill. However, although clause 47 of the IP Bill provides that the interception of communications in a prison is authorised if it is conduct in exercise of any power conferred by or under Prison Rules, there is no provision for oversight of the operation of those powers. Clause 205 of the IP Bill sets out the main oversight functions of the Investigatory Powers Commissioner and includes the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc.) and the exercise of functions by virtue

28 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF

of sections 1 to 4 of the Prisons (Interference with Wireless Telegraphy) Act 2012. Both of these functions are new areas of oversight which we have so far informally been asked by the Home Office and Ministry of Justice to oversee. It seems odd that these two new areas of oversight are included in the IP Bill, but there is no explicit provision for our current oversight of the interception of communications in prisons. To remedy this, clause 206 of the IP Bill requires amending to include oversight of conduct taking place under Chapter 2 of Part 2 of the IP Bill.

**5.23** Although we welcome a number of the amendments which have already been made by the Government to the IP Bill, in our view there is still room for further amendments to enhance safeguards and to increase accountability and transparency.

# Section 6
# Interception of Communications

**6.1** In this section we 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 IOCCO's inspections.

**6.2** Before doing so, it is worth pointing out that we are constrained by the statutory secrecy provisions in section 19 of RIPA forbidding disclosure of certain aspects of interception, for example, the existence and contents of a warrant, the steps taken in pursuance of a warrant, and everything in the intercepted material, together with any related communications data. Because of this it is challenging to provide a full public account of the interception that is undertaken.

## Interception Legislation

**6.3** Chapter 1 of Part 1 of RIPA (sections 1-20) covers the interception of communications. The Interception of Communications Code of Practice[29] provides detailed guidance on the procedures that must be followed by public authorities before interception of communications can take place under the provisions of RIPA. Unless otherwise stated, references in this section to the Code of Practice mean the Interception of Communications Code of Practice.

**6.4** Section 72 of RIPA states that public authorities must have regard to the provisions of the Code of Practice but that a failure on the part of any person to comply with any provision of a Code of Practice shall not of itself render him liable to any criminal or civil proceedings.

## Applications for Interception Warrants

**6.5** Part 1 of RIPA provides that the interception of communications may be authorised by 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 2 of Part 1 of RIPA).

**6.6** **The 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, 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) on behalf of the

29 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf

NCA and all UK police forces;

- the Commissioner of the Metropolitan Police Service (MPS);
- 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, Ministry of Defence (MOD).

**6.7 Secretaries of state.** Interception warrants have to be authorised by a secretary of state (sections 5(1) and 7(1)(a) of RIPA). He or she has to sign the warrant personally, or in an urgent case may authorise the issue of a warrant signed by a senior official (section 7(1)(b) of RIPA).

**6.8** 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.[30]

**6.9** Each secretary of state has senior officials and staff in their warrant issuing department. Their functions include scrutinising warrant applications for their form, content and sufficiency, and presenting them to the secretary of state with appropriate recommendations.

**6.10 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;[31]
- for the purpose [in circumstances appearing to the secretary of state to be relevant to the interests of national security][32] 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)).

30 Interception warrants to prevent or detect serious crime may be authorised by Scottish Ministers, under the Scotland Act 1998. In this report references to "secretary of state" should be read as including Scottish Ministers where appropriate. The functions of the Scottish Ministers also cover renewal and cancellation arrangements.

31 Section 81(3) of the Act 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.

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

**6.11** These statutory purposes and the requirement of necessity are derived directly from Article 8 of the ECHR. To issue an interception warrant for any other purpose would be unlawful. It is part of IOCCO's function to make sure that all warrants are issued for these statutory purposes only.

**6.12** **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.

**6.13** Proportionality pervades human rights jurisprudence and is a thread which runs through RIPA. 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 not applied for, where it is judged that the necessity does not outweigh the intrusion.

## Interception Warrants

**6.14** All interception warrants are for the interception of the content of communications and the acquisition of related communications data.

**6.15** Applications for interception warrants should contain the information included in Paragraph 5.2 or 6.10 of the Code of Practice. Applications contain detailed explanations and supporting information including specific sections on the protection of privacy, to help the secretary of state assess the merits of the application.

**6.16** Interception warrants have an initial duration of six months where the statutory purpose is national security or economic well-being but three months where the statutory purpose is serious crime (section 9(6) of RIPA). They cease to have effect at the end of their period unless they are renewed.

**6.17** The secretary of state may renew an interception warrant only if he or she believes that it continues to be necessary for a statutory purpose (section 9(2) and Paragraphs 5.15 and 6.23 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.

**6.18** 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 Paragraphs 5.17 and 6.25 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, the responsibility to cancel a warrant is exercised on

behalf of the secretary of state by a senior official in the warrant issuing department.

**6.19** Exceptionally a warrant may be issued in an urgent case by a senior official but only if it is expressly authorised by a secretary of state (sections 7(1)(b), 7(2)(a) of RIPA and Paragraphs 5.6 and 6.16 of the Code of Practice). An urgent warrant lasts for five working days unless it is renewed by the secretary of state (section 9(6)(a) of RIPA).

**6.20** Interception warrants may be issued under the provisions of either section 8(1) or section 8(4) of RIPA.

**6.21** **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. The definition of "person" in section 81(1) includes any organisation and any association or combination of persons.

**6.22** An application for a section 8(1) warrant should contain the details required by Paragraph 5.2 of the Code of Practice. The required details include:

- the background of the operation;
- the person or premises constituting the subject of the application (and how the person or premises features in the operation);
- a description of the communications to be intercepted, details of the CSPs and an assessment of the feasibility of the interception operation where this is relevant;
- a description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data. This conduct may include the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a);
- an explanation of why the interception is necessary under section 5(3);
- consideration of why the conduct is proportionate to what is sought to be achieved by that conduct;
- consideration of any collateral intrusion and why that intrusion is justified in the circumstances;
- whether the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between an MP and another person on constituency business;
- where an application is urgent, the supporting justification;
- an assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of RIPA.

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

**6.24** **Section 8(4) interception warrants**. Section 8(4) warrants are for the interception of external communications, namely those sent or received outside of the British Islands[33] (see section 20 of RIPA for a definition of external communications). 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. Section 8(4) does not impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

**6.25** 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 gives 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) of RIPA.

**6.26** By virtue of section 8(5)(b) an interception warrant may also authorise other conduct as described in section 5(6) of RIPA. Such conduct includes the interception of communications not identified in the warrant the interception of which is necessary in order to do what the warrant expressly authorises. Therefore in principle a section 8(4) warrant can include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates. When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the secretary of state under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications.

**6.27** A application for a section 8(4) warrant should contain the details required by Paragraph 6.10 of the Code of Practice. The required details include:

- the background of the operation;
- a description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant;
- a description of the conduct to be authorised, which must be restricted to

33 The United Kingdom of Great Britain & Northern Ireland, the Channel Islands and the Isle of Man.

the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data;

- 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 to what is sought to be achieved by that conduct;
- where an application is urgent, supporting justification;
- 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; and
- an assurance that all intercepted material will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA.

**6.28** 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 1 of Part 1 statutory purpose. Examination of material for any other purpose would be unlawful.

**6.29** **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. 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.

**6.30** **Additional safeguards for section 8(4) interception warrants.** There are extra safeguards in section 16 of RIPA 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 statutory purpose under Chapter 1 of Part 1 of RIPA, 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.

**6.31** Thus a section 8(4) warrant does not generally permit the 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).

**6.32** Section 16(3) of RIPA 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 six months for national security purposes or

three months for serious crime or economic well-being purposes. Since this certification has to relate to an individual, it is broadly equivalent to a section 8(1) warrant.

**6.33** Sections 16(4) and (5) of RIPA 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 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.

**6.34** **Selection of section 8(4) material**. 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 requirement), and why such access is proportionate. Our inspections and audits show that the selection procedure is carefully and conscientiously undertaken both in general and, so far as we are able to judge, by the individuals concerned. The procedure relies mainly on the professional judgment of analysts, their training and management oversight. However, separate pre-authorisation by a more senior operational manager is required for the targeting of communications regarded as confidential under the Code of Practice. All staff are required to undertake and pass a test at least once every two years to demonstrate their continuing understanding of the legal and other requirements.

**6.35** The Commissioner is responsible under section 57(1)(d) for reviewing the adequacy of the arrangements as a whole under section 15 (and 16) of RIPA. GCHQ's Internal Compliance Team and staff under their direction, conduct audit checks on a randomised sample of the analysts' justifications for selection. 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 IOCCO during our inspections and any breaches of the section 15 and 16 safeguards will have already been reported to IOCCO (see the errors section of this section). The retrospective audits are a strong safeguard and also serve to act as a deterrent against malign use. Later in this section we set out some of the changes we have made to our interception inspection regime, one of which relates to our involvement in the audit process.

**6.36** There are a number of other security and administrative safeguards in place within GCHQ (which are not only relevant to interception work). These include the security policy framework (including staff vetting), the continuing instruction and training of all relevantly engaged staff in the legal and other requirements of RIPA, 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.

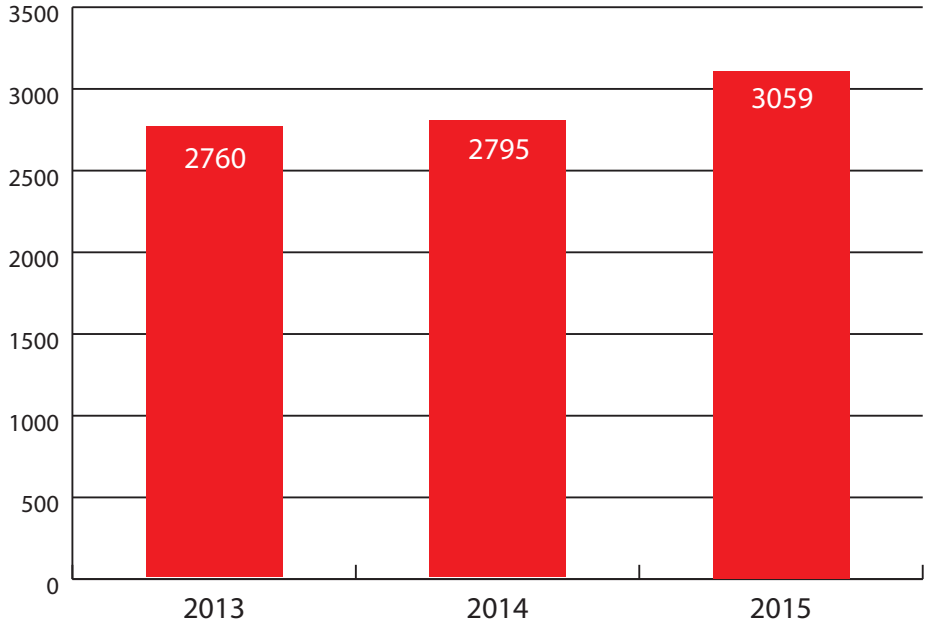
## Statistics for Interception Warrants

**6.37** There are no statistical requirements in the Code of Practice. For some time we have highlighted this fact and made clear that we would welcome the inclusion of statistical requirements into the Code of Practice to improve transparency and accountability in this area.[34] In the absence of any codified requirements, we have worked with the interception agencies and warrant issuing departments, to provide some statistical information about how the powers under Chapter 1 of Part 1 of RIPA are being used.

**6.38** **Figure 2** shows the number of new interception warrants issued in each of the years 2013-2015 for the nine interception agencies. The total number of warrants issued during 2015 was 3059, an increase of 9% on 2014.

**6.39** **Figure 3** details the breakdown by statutory necessity purpose of the 3059 interception warrants issued in 2015. The combination category represents those few warrants that were authorised for more than one statutory purpose. The vast majority of the serious crime warrants fall into one of the following five categories: unlawful supply of controlled drugs, firearms, financial crime (such as money laundering), armed robbery and human trafficking.

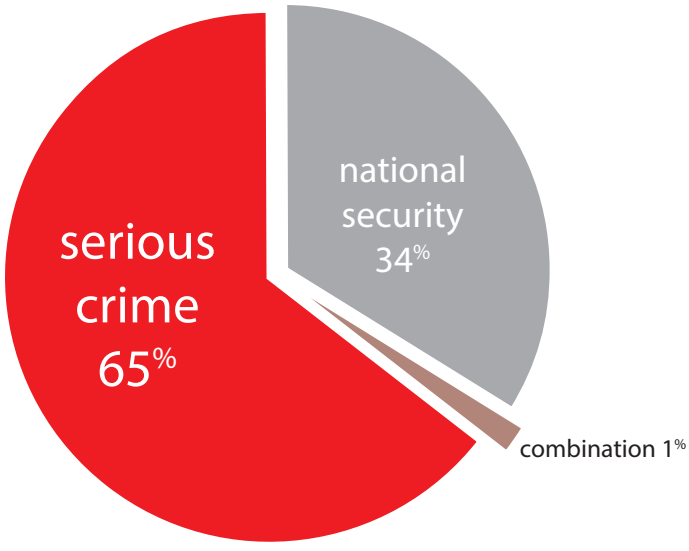
**Figure 2** *Total number of interception warrants issued 2013-2015*




34 See for example our evidence to David Anderson QC http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf and our evidence to the Joint Committee scrutinising the Investigatory Powers Bill http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20IP%20Bill%20Joint%20Committee.pdf.

**6.40** Some 80 of the 3059 warrants (approximately 2.5%) were approved urgently by the secretary of state under the hand of a senior official. These warrants all related to exceptionally urgent cases where, for example, there was an imminent and credible threat to life or limb within the next 24 hours; an imminent and credible threat to national security or a unique opportunity to obtain intelligence or to prevent loss of intelligence of vital importance to national security; an imminent importation or handover within the next 24 hours of a substantial quantity of drugs; or a unique opportunity to obtain intelligence of vital importance in relation to preventing or detecting serious crime. The majority of those urgently approved were issued on behalf of the Security Service or the NCA.

**Figure 3** *Warrants issued by statutory purpose in 2015*




**6.41** We previously commented that the rejection figure for interception warrants is inevitably low due to the high level of scrutiny that is applied to each warrant application as it crosses a number of desks in the interception agency and the relevant warrant issuing department before it reaches the secretary of state. This year we asked the interception agencies and warrant issuing departments to capture statistical information relating to the number of warrants that were subject to challenge or further information requests by the senior official or secretary of state prior to their being approved, or that were rejected by the secretary of state. They reported to us that on 64 occasions a senior official or secretary of state called for further information prior to approving a warrant. On six occasions a secretary of state refused an interception warrant. It is important to note that these figures cover a mixture of new warrant applications, modifications and renewals and so the figure should not be taken as a percentage of the 3059 warrants issued in 2015. It is also important to note that this figure does not capture the guardian and

gatekeeper / quality assurance function carried out by first the staff and lawyers within the interception agency responsible for reviewing all submissions (prior to them being forwarded to the warrant issuing department), or, secondly, the guardian and gatekeeper / quality assurance function carried out by staff in the relevant warrant issuing department prior to the warrants submission to the senior official and secretary of state.

**6.42** The total number of warrants in force on 31 December 2015 was 1518, a 5% decrease on 2014. Of the 1518 warrants in force on 31 December 2015, 22 were issued under section 8(4) of RIPA. Some of the 1518 warrants were first authorised before 2015 but the vast majority of interception warrants do not run for longer than six months.

## Inspection Regime

**6.43** **Objectives of Inspections.** IOCCO's interception inspections are structured to scrutinise the key areas covered by Chapter 1 of Part 1 of RIPA and the 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 Chapter 1 of Part 1 of RIPA and that all relevant records have been kept;
- examination of selected interception applications to assess whether they were necessary in the first instance and whether the requests met the requirements of necessity and proportionality;
- interviews with case officers, analysts 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 that 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;
- a review of the adequacy of the safeguards and arrangements under section 15 (and 16) of RIPA;
- 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.

**6.44** After each inspection IOCCO 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 issuing department.

**6.45** IOCCO's inspections of the four main warrant issuing departments have a slightly different emphasis. The warrant issuing departments undertake an important function which is comparable to the guardian and gatekeeper role performed by the SPoC for communications data applications under Chapter 2 of Part 1 of RIPA. Warrant issuing departments 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 warrant issuing department 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. After each inspection of a warrant issuing department IOCCO compiles a detailed inspection report and action plan setting out the findings and recommendations. The report is sent to the head of the warrant issuing department (senior official) and is copied to the relevant secretary of state.

**6.46** **Inspection Reports.** IOCCO's reports contain formal recommendations with a requirement for the interception agency or warrant issuing department to inform IOCCO within two months on the progress that has been made. The inspection reports include:

- an assessment of the extent to which the recommendations from the previous inspection have been achieved;
- a summary of the number and type of interception documents selected for inspection, including a detailed list of those warrants;
- detailed comments on all warrants selected for further examination and discussion during the inspection;
- an assessment of the errors reported to IOCCO 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 warrant issuing departments raised with IOCCO during the inspection;
- an assessment of how any material subject to legal professional privilege (or otherwise confidential material) has been handled;
- a number of recommendations aimed at improving compliance and performance generally;
- an overall assessment of the interception agency's or warrant issuing department's level of compliance with RIPA.

**6.47** We shall describe some of the most frequent recommendations and a number of other matters arising from the inspections later in this section of the report.

**6.48** **Number of inspections.** In 2015 IOCCO maintained the pattern of inspecting all nine interception agencies and the four main warrant issuing departments 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 two or three and take place over three days. The inspections of the smaller volume users are generally conducted by an inspection

team of two and generally last one or two days. As a point of principle we inspect each warrant issuing department after the interception agencies for which it is responsible. This provides an opportunity for us to discuss the findings and recommendations from the interception agencies' inspections with the warrant issuing departments. 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 or breaches.

**6.49 Examination of warrants.** IOCCO 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 we select warrants 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 that 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.
- Secondly, we scrutinise the selected warrants and associated documentation in detail during reading days which precede the inspections.
- Thirdly, 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. Where necessary we require and examine further documentation or systems in relation to those matters.

**6.50 Samples.** The total number of warrants individually examined during the 26 interception inspections was 1148. This figure equates to three quarters of the number of warrants in force at the end of the year and three eighths of the total new warrants issued in 2015.

**6.51 Audits and query based[35] examinations.** We have unfettered access to the application and authorisation systems in place within a number of the interception agencies and in those cases 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 examinations against the material and reports.

**6.52** These examinations give insight into the use of the material, 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. In a scientific sense, we test the operational hypothesis set down in the initial application that was authorised as we are able to examine within the operational environment the interference. These

35 Query based examinations involve searches against defined criteria or subjects.

are all important components of the review and re-assessment of the necessity and proportionality of the conduct authorised and compliance with the legislation.

**6.53** 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 Article 8 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, if it did so 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 / breaches resulted from the interference or intrusion.

**6.54** For example, we might conduct a query based examination to check that the intercepted material has been examined in a timely fashion, or to scrutinise the intelligence value or 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 examinations on keywords (e.g. "solicitor", "legal") to identify cases where communications subject to legal privilege may have been intercepted and retained. We are 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.

**6.55** In a large number of instances we conduct this audit between renewals. This enables us to reassess the necessity and proportionality of the conduct authorised and to review whether the conduct was foreseen by the person authorising the application. As a result of our observations we have in a number of cases recommended the warrant's modification, required changes to operational practice to safeguard privacy, required additional information to be provided to the secretary of state immediately or at the point of next renewal, or recommended cancellation.

**6.56** This audit function is easily achievable with the majority of the law enforcement 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 we have no statutory function to oversee. We have made arrangements to view the applications electronically in one of the intelligence agencies and later in the report we set out a number of changes that we will make to the inspection regime in 2016 to bring about increased scrutiny and oversight to other parts of the process.

**6.57** **Retention, storage and deletion of intercepted material and related communications data.** Each interception agency has a different view on what constitutes an appropriate retention period for intercepted material and related communications data. There is no period prescribed by the legislation, but the agencies must comply with section 15(3) of RIPA which provides that the material or data must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes in section 15(4) of RIPA.

**6.58** In 2013/14 we conducted an audit of the retention, storage and deletion of intercepted material and related communications data during which we examined the interception agencies' systems and policies in place.[36] This audit concluded that indiscriminate retention for long periods of unselected intercepted material (content) does not occur and that the interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of RIPA. We identified that related communications data are in some instances retained for a variety of longer periods and made 22 recommendations in 2013 and 11 in 2014 for the interception agencies to review or shorten their retention periods and / or destroy intercepted material (and related communications data) where there was no persuasive justification provided for its ongoing retention. We can report that all of the recommendations have now been implemented by the interception agencies. The recommendations caused a significant amount of material and related communications data to be destroyed, and in some instances entire systems have been decommissioned.

**6.59** The majority of content is reviewed and automatically deleted after a short period of time unless action is taken to retain the content for longer because it is necessary to do so. The retention periods for selected content differ within the interception agencies but range from between 30 days to one year. The retention periods for related communications data also differ within the interception agencies but range from between six months and one year.

**6.60** It is important for the agencies' retention and destruction policies to 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. On an annual basis we require an update on any changes to the retention, storage and deletion arrangements for systems containing intercepted material and related communications data. In 2015 a number of interception

36 See Paragraphs 3.48 to 3.57 of our 2013 annual report http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf and Paragraphs 6.60 to 6.65 of the 2014 Annual Report http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

agencies notified us of their intention to make minor amendments to their systems or informed us that they had decommissioned certain legacy systems.

**6.61** **Retention of interception applications and associated documentation.** In 2015 we carried out a review of the procedures in place for the retention of interception applications and associated documentation (for example, renewals, modifications, cancellations, instruments and schedules) by the interception agencies, warrant issuing departments and CSPs. There is no explicit provision in RIPA or the Code of Practice requiring the destruction of warrantry applications and associated documentation. Conversely, there is no express requirement for retention. That said, if an application or renewal contains information that discloses it to be the product of warranted interception, the document may well fall within section 15(3) of RIPA.

**6.62** We found, unsurprisingly given the lack of specific provisions in RIPA and the Code of Practice, a variety of different retention arrangements within each of the interception agencies, warrant issuing departments and CSPs. Some of the interception agencies, warrant issuing departments and CSPs retain this documentation indefinitely whereas others, mostly the law enforcement agencies, destroy them within a reasonable period of time after the interception has been cancelled and any legal proceedings have ended.

**6.63** For inspection purposes we would be content for the records to be retained by the interception agencies and warrant issuing departments for up to two years after the individual interception warrant had been cancelled. For CSPs, we do not see the need for the documentation to be retained after the interception has been cancelled. However another important consideration relates to ensuring the documentation is retained for a sufficient period to enable the IPT to exercise its jurisdiction. Section 67(5) of RIPA provides that the IPT shall not consider or determine any complaint if it is made more than one year after the conduct to which it relates unless it is equitable to do so. Some of the interception agencies or warrant issuing departments cited duties under the relevant Public Records Acts to retain documentation indefinitely. A number of the interception agencies or warrant issuing departments asked for guidance on whether they should keep the records in hard copy or whether they could be scanned and retained electronically. We have no preference provided it is possible to sufficiently identify the provenance of any scanned or electronic copies. It would be helpful if the Code of Practice clarified these matters. We note that Paragraph 10.1 of the draft IP Bill Code of Practice for the Interception of Communications states that *"It is desirable, if possible, to retain records for up to five years."* This provision would benefit from further clarity, in particular, whether it is permissible to retain documents indefinitely.

## Inspection Findings & Recommendations

**6.64** The total number of recommendations made in our inspection reports for the nine interception agencies was 55, an average of six per interception agency. The number of recommendations made in our inspection reports to the warrant issuing departments was 19, an average of five per warrant issuing department.

**6.65** 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 (in submissions) to the secretary of state or senior official. 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.

**6.66** **Figure 4** shows that 77% of the recommendations emanating from the inspections fell into three key categories: Application Process, Authorisation / Implementation of Warrants or Procedures.

### Application Process

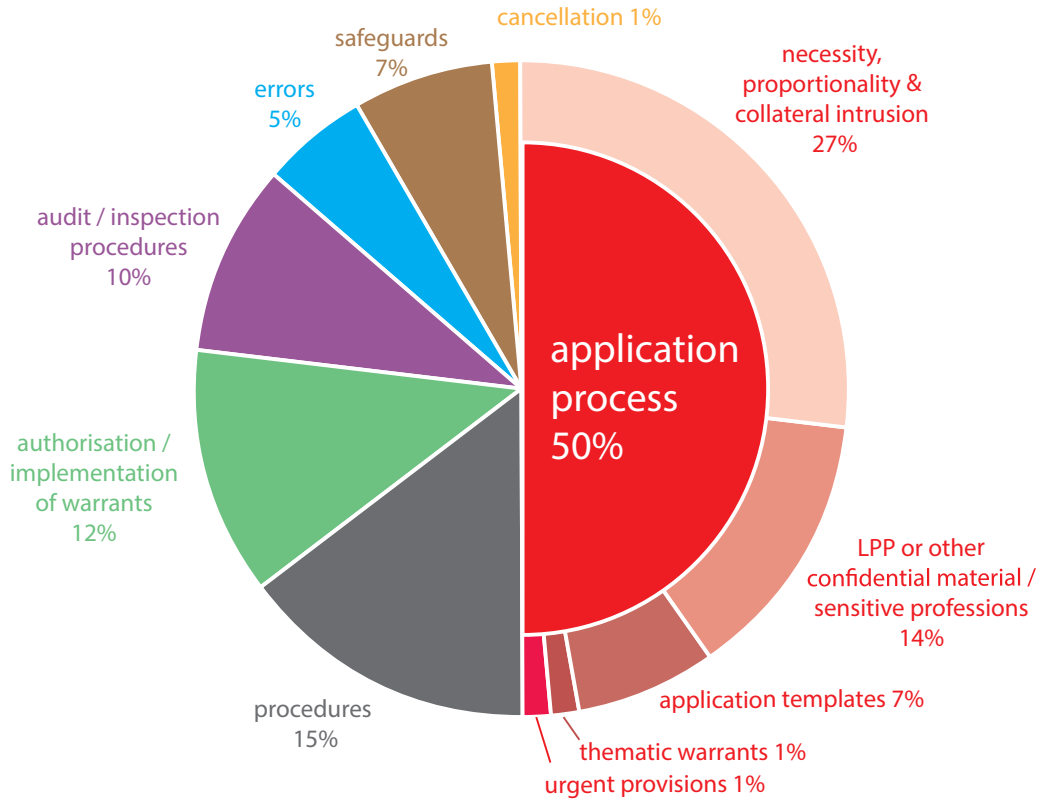
**6.67** Some 50% of the 74 recommendations were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality or collateral intrusion justifications in the applications, the handling of material subject to legal professional privilege or otherwise confidential material, or considerations regarding sensitive professions.

**6.68** **Necessity, proportionality and collateral intrusion.** A key part of the necessity test is to make the link between the individual under investigation, the identifier 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 or threat to national security was or explicitly state what were the potential criminal offences (i.e. relevant legislation) that the agency was trying to prevent or detect. The latter was prevalent where interception was being conducted primarily for strategic preventative purposes or where the warrants related to investigations undertaken by police force Professional Standards Departments (PSDs).

**6.69** Last year we made a number of recommendations to the interception agencies to ensure that renewal submissions contain a considered assessment of the actual intrusion (whether collateral or otherwise) and how effective the steps to minimise that intrusion have been. Generally we were satisfied this year that there had been improvements in this respect, although we made one recommendation in this area for a warrant issuing department to exercise a more robust guardian and gatekeeper role in this respect. We

were pleased to note greater emphasis in submissions on the steps (including technical or other filters) that would be put in place to minimise collateral intrusion, particularly where the communications identifiers were likely to be used by individuals who were not of intelligence interest. The recommendations in these areas this year were more precise and were limited to a small number of the submissions examined, rather than being broader issues.

**Figure 4** *Interception recommendations by category*




**6.70 Legal professional privilege material or otherwise confidential material / sensitive professions.** There are special arrangements and safeguards in the Code of Practice on these matters. Intercepting communications involving legal professional privilege or confidential journalistic or personal material gives rise to issues under Article 6 (right to a fair trail) of the ECHR and Article 10 (freedom of expression), as well as Article 8 (right to privacy).

**6.71** We made a number of recommendations where material subject to legal professional privilege or otherwise confidential material (such as confidential journalistic

material or confidential personal information) had been incidentally obtained. The recommendations required renewal submissions to make reference to instances where such material had been intercepted and to explain how the material had been handled. In the vast majority of cases the material was immediately destroyed because it was of no intelligence interest. However, where such material had been retained, it was brought to our attention in accordance with the Code of Practice. Recommendations were made for managers to carry out regular reviews of such intercepted material in order to ensure compliance with the safeguards.

**6.72** In the small number of cases where the subject of the interception was (or was believed to be) a member of a sensitive profession (e.g. a journalist, lawyer or medical doctor) the applications gave consideration to the potential of obtaining confidential information or material subject to legal professional privilege. However it was not always explicit whether the intention was to acquire this type of material or whether consideration was being given to the likelihood of obtaining such material incidentally. We made appropriate recommendations in this respect.

**6.73** **Application templates.** An application for an interception warrant should contain the details required by Paragraph 5.2 or 6.10 of the Code of Practice. The Home Office published a national application template for communications data under Chapter 2 of Part 1 of RIPA, but has not done the same for interception. As a result, the nine interception agencies have developed their own application templates. The Security Service and the law enforcement agencies (HMRC, PSNI, Police Scotland, MPS and the NCA) have more structured templates which guide the applicants through the requirements. We have recommended that GCHQ and SIS work with the Foreign and Commonwealth Office (FCO) to design and implement more structured application templates and warrantry documentation. We favour national templates in order to achieve consistency in requirements and standards across the nine interception agencies and warrant issuing departments as do the CSPs.

## Authorisation / Implementation of Warrants

**6.74** 12% of the recommendations related to the authorisation or implementation of interception warrants. These included recommendations to improve the audit trail for warrants issued orally under the authority of a secretary of state and to ensure that any early reviews requested or restrictions placed on warrants by the secretary of state were captured and actioned.

## Procedures

**6.75** 15% of the recommendations were made for the interception agencies or warrant issuing departments to make clearer their procedures or policies relating to certain matters, for example, emergency authorisations or the handling of legal professional privilege or other confidential material. The latter matters required revision after key judgments in cases before the IPT (i.e. Chatwani & Others vs. the National Crime Agency

and Belhadj and Others vs. the Security Service, SIS, GCHQ, Home Office and FCO) and in light of draft amendments that were made to the Code of Practice.

**6.76** Overall we found good progress against the recommendations we made in 2014. In particular we welcomed the introduction of additional signing slots with the secretaries of state during recess periods, improvements in the timescales within which instruments, modifications and cancellations are served on CSPs, the implementation of the recommendations relating to the retention, storage and destruction of intercepted material and related communications data, and those relating to collateral intrusion and filtering techniques.

## Changes to the Interception Inspection Regime

**6.77** During the past three years we have made a number of significant improvements to and strengthened the interception inspection regime, as we have mentioned in previous reports.[37]

**6.78** In 2015 we decided to make a number of further changes to the interception inspection regime from January 2016. The first change is to move from bi-annual to annual inspections of the warrantry processes at all interception agencies and warrant issuing departments. This change will bring the interception regime in line with our communications data regime under Chapter 2 of Part 1 of RIPA. It will enable us to conduct more ad hoc thematic inquiries, investigations and reviews throughout the year and allow us to implement a phased inspection programme for GCHQ where the scale and complexity of the interception activity undertaken necessitates a different inspection approach. The change from bi-annual to annual inspections of the warrantry process will not lead to any reduction in oversight as we intend to scrutinise the same percentage of warrantry documentation on an annual basis.

**6.79** GCHQ is unique in terms of the type and scale of the interception it undertakes and therefore it is necessary to take a different inspection approach with the GCHQ inspections to ensure the process is audited from end to end. Moving to a phased inspection model will enable us to concentrate in more detail on key themes and provide independent verification of the end to end process. We have proposed a 5-phase inspection model for GCHQ. It is our intention in 2016 to conduct a formal inspection on each of the five phases and to arrange ad hoc visits in-between, when necessary, for example, to carry out thematic reviews, audits or error investigations. The five phases are as follows:

**6.80** Phase 1: Warrantry process – This phase will broadly cover an evaluation of the systems in place for the interception of communications to ensure they are sufficient; an examination of selected interception applications to assess whether they met the requirements of necessity and proportionality; interviews with case officers, analysts and / or linguists from selected investigations or operations to assess whether the interception

37 For example see Paragraphs 6.61 to 6.65 of our March 2015 report http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

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 interception.

**6.81** Phase 2: GCHQ Audits – This phase will cover scrutinising the results of the audits conducted by GCHQ on systems containing intercepted material and related communications data (as mentioned earlier in this section of the report). IOCCO will also now participate in some of the system audits to provide independent verification.

**6.82** Phase 3: Safeguards - On an annual basis IOCCO will require an update on any changes to the retention, storage and deletion arrangements for systems containing intercepted material and related communications data and will scrutinise those changes to ensure compliance with section 15 of RIPA. For some time we have said that we would benefit from additional technical resource. The creation of an Investigatory Powers Commission under the IP Bill would provide the opportunity to ensure this technical resource is secured. Once the technical resource is in place IOCCO will seek to conduct visits to collection sites and to examine the selection and filtering processes and technical systems in more detail with a view to independently verifying that the interception being carried out accords with the authorisation and that the intrusion and collection of incidental material is minimized as far as is technically possible. In addition IOCCO will be briefed on (or attend) training courses that are provided to GCHQ staff on RIPA related matters. GCHQ also suggested some further elements to supplement phase 3 in the form of additional briefings and demonstrations to enable deeper consideration of the complex end to end interception process.

**6.83** Phase 4: Sharing of intercepted material and related communications data with international partners – We commissioned an investigation in 2015 into the arrangements in place within GCHQ for the sharing of intercepted material and related communications data with foreign partners in order to review compliance with the section 15 safeguards. We are still in the process of carrying out this investigation. Once our in-depth investigation has been completed we will require an annual update on any changes or new arrangements. This is an area we have been discussing with our international counterparts.

**6.84** Phase 5: Error investigations: We will require annual analysis of any trends or patterns in errors and a review of the measures put in place to prevent recurrence. On an ad hoc basis IOCCO would seek to continue to investigate in more detail any significant technical or otherwise serious errors.

**6.85** We will provide an update in our 2016 report as to the implementation and findings relating to this new five phase inspection regime.

## Interception Errors

**6.86** The Commissioner has a duty under sections 58(2) and (3) of RIPA to report to the Prime Minister any contravention of the provisions of RIPA, or any inadequate discharge of section 15 safeguards.

**6.87** In our last annual report we noted that there was no provision for error reporting in the Code of Practice, unlike the clear provisions in the Acquisition and Disclosure of Communications Data Code of Practice. Error reporting is an important part of the oversight regime and aids accountability and public confidence. It is vital to ensure consistency of approach from all interception agencies in terms of thresholds, judgments and reporting criterion for errors. We welcome efforts in the IP Bill and the draft IP Bill Code of Practice for the Interception of Communications to define an error and introduce error reporting procedures. However we have a number of concerns with the adequacy of these provisions and have suggested amendments as set out in our various evidence submissions and in **Section 5** of this report.

**6.88** We have for some time raised concerns with a number of the interception agencies about the timeliness of the submission of error reports to IOCCO. In 2015 GCHQ had a significant backlog in their error reports. Although it is appreciated that due to the complexity of the different collection and selection systems at GCHQ it sometimes takes longer to investigate the cause of errors and to put systems and procedures in place to prevent recurrence, a number of the errors that they were slow to report were fairly simple one-off human errors and in our view there should be no reason for those reports to be delayed significantly. GCHQ has worked hard to reduce the backlog by streamlining their error reporting process and by allocating more resources to the central team who deal with the investigation and reporting of errors. There is still more work to be done to speed up the reporting time and it is important for the IP Bill Interception of Communications Code of Practice to provide a defined timescale for errors to be reported.

**6.89** Last year we mentioned that an interpretation issue had arisen with regard to instances where an interception agency applies for a warrant in good faith and exercises due diligence to check that the identifier is being used by the subject of interest but where the identifier turns out not to be used by the person expected. We would expect such instances to be reported to us as, even though the interception of the identifier was authorised by the secretary of state and so arguably there was no contravention of RIPA, the conduct did result in intrusion into the privacy of an individual who was not of intelligence interest and for whom the secretary of state did not consider the necessity or proportionality case. The fact that such occurrences are unintentional and are not generally the result of some direct or deliberate action or other failure does not mean that they should not be reported to us. The Commissioner rejects the suggestion that interception which infringes on the privacy (or other) rights of an individual who was not the subject of interest should not be reported on the grounds that the intrusion was unintentional. We understand why the agencies are reluctant to classify these instances as "errors" and agree these occurrences might better be described as "reportable instances". It is important that the IP Bill Code of Practice for the Interception of Communications

provides clarity on these matters and the interception agencies and warrant issuing departments should work with the Home Office and the Commissioners from the current oversight bodies to achieve this. The agencies should also take steps to reinforce with transcribers and operational teams the importance of identifying promptly when a subject of interest is not using a particular identifier, ensuring that the interception is suspended and cancelled immediately and that such instances are reported to IOCCO.

## Error statistics

**6.90** The total number of interception errors reported to IOCCO during 2015 was 62. The breakdown of the causes of the errors is contained in **Figure 5**.

**6.91** Some 76% of the errors were attributable to the interception agencies and 13% to the CSPs when giving effect to interception warrants.

**6.92** The remaining 11% of the interception errors were caused by CSPs providing police forces with the content of communications when only communications data under Chapter 2 of Part 1 were required or contraventions of section 1(5) of RIPA, for example, where police forces did not have the necessary authority in place to access stored communications (see sections 2(7) and 2(8) of RIPA for definition of stored communications).

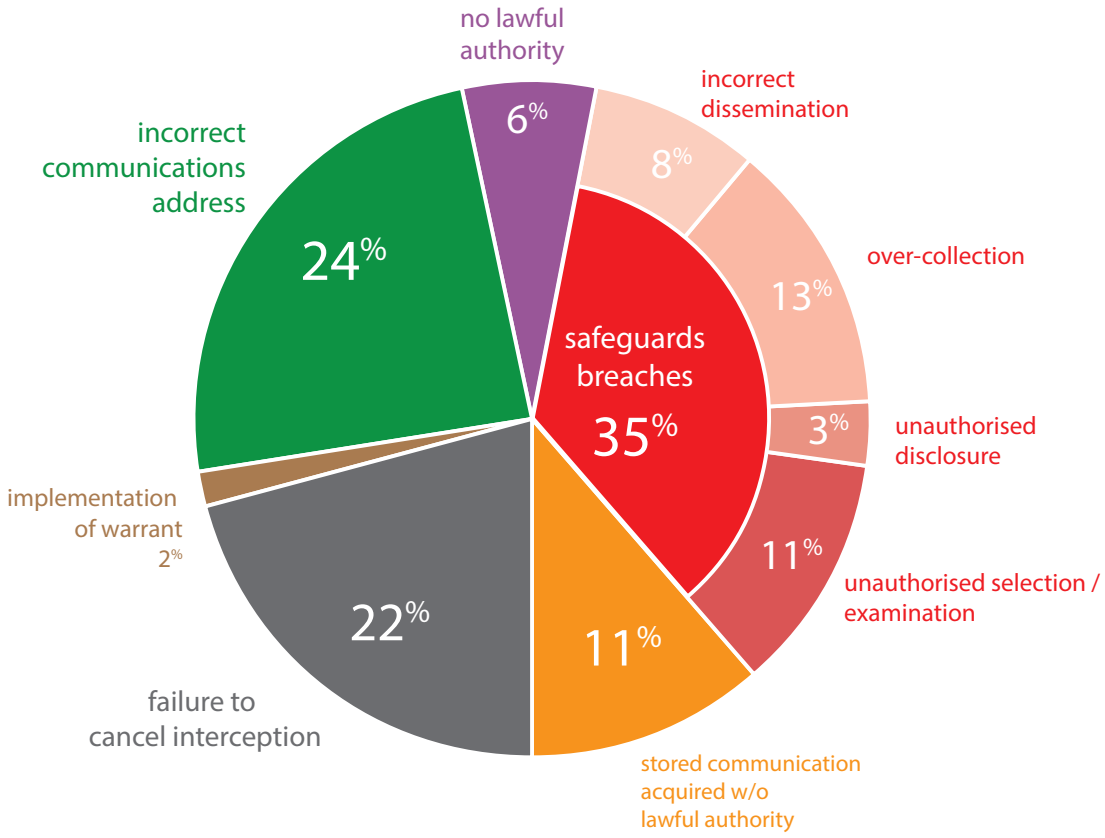
**6.93** **Figure 5** shows that 81% of reported errors fell into three key categories: section 15/16 safeguards breaches, failure to cancel interception or interception of the incorrect identifier. This is an almost identical pattern to 2014.

## Section 15/16 safeguards breaches

**6.94** Some 35% of the errors constituted breaches of the section 15/16 safeguards. The majority of errors in this category fell into three distinct areas and some examples of these errors are given here.

**6.95** **Over-collection.** These were generally 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 (e.g. 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 (for example, machine to machine). 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.

**Figure 5** *Breakdown of interception errors by cause*




**6.96** **Unauthorised selection / examination.** The most common errors in this category were instances where an analyst mistakenly continued to select the communications of an individual based overseas after the individual was known to have entered the UK or technical failures which led to the incorrect selection of material or material continuing to be selected after it had been de-tasked.

**6.97** **Incorrect dissemination.** These error instances constitute non-compliance with section 15(2) of RIPA. They were mainly 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

**6.98** 22% 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 results as the material is stopped from entering the interception agency or is immediately discovered by system administrators and deleted.

### Incorrect communications address intercepted

**6.99** 24% of the errors were caused as a result of the incorrect identifier being intercepted. The majority of these were human errors. In some cases there was an inadvertent transposition of the identifier by the interception agency when applying for the warrant or by the CSP when effecting the interception. 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 incorrect. In the majority of cases the staff conducting the interception detected these errors promptly and the interception was immediately suspended and then cancelled.

**6.100** The interception agencies and CSPs provided IOCCO 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 any erroneously acquired material or data that was not of intelligence interest was destroyed.

# Points of Note

### Interception of Communications

3059 interception warrants (to access the content of communications and related communications data) were issued in 2015. Approximately 2.5% of those warrants were approved urgently.

65% of the 3059 warrants were issued for the purpose of the prevention or detection of serious crime, 34% in the interests of national security and the remaining 1% for a combination of purposes.

1518 interception warrants were extant on 31 December 2015. Of those, 22 were issued under section 8(4) of RIPA.

In 2015 IOCCO conducted 26 interception inspections. During these inspections 1148 interception warrants were examined which equates to three quarters of the number of extant warrants at the end of the year or three eighths of the new warrants issued in 2015.

The total number of recommendations made in our inspection reports for the nine interception agencies and four warrant issuing departments was 74. The majority of recommendations fell into three key categories – application process, authorisation / implementation of warrants and procedures.

We also carried out a review of the retention of interception applications and associated documentation and found, unsurprisingly given the lack of specific provisions in RIPA and the Code of Practice, a variety of different arrangements within the interception agencies, the warrant issuing departments and the Communication Service Providers (CSPs).

62 interception errors were reported to IOCCO in 2015. 81% of the errors fell into three main categories: section 15/16 safeguards breaches, failure to cancel interception, or interception of the incorrect identifier.

Building upon the significant improvements that we have made over recent years to our interception inspection regime we have decided in 2016 to move from bi-annual inspections of the warrantry process to annual inspections. The same volume of applications will be examined during the inspections and so there will be no less scrutiny of the warrantry process. However this will free up more time for us to carry out thematic inquiries, investigations and reviews, and enable us to implement a five-phase inspection programme for GCHQ which reflects the scale and complexity of the interception activities GCHQ undertakes.

# Section 7
# Communications Data

**7.1** In this section we provide an outline of the communications data legislation, give details of the communications data inspection regime, provide statistical information about the use of communications data by public authorities and outline the key findings from IOCCO's inspections.

## Communications Data Legislation

**7.2** Chapter 2 of Part 1 of RIPA (sections 21 to 25) and the Acquisition and Disclosure of Communications Data Code of Practice[38] made under section 71 of RIPA concerns the procedures for the acquisition and disclosure of communications data. Unless specified, references in this section to the Code of Practice mean the Acquisition and Disclosure of Communications Data Code of Practice.

**7.3** Section 72 of RIPA states that public authorities must have regard to the provisions of the Code of Practice but that a failure on the part of any person to comply with any provision of a Code of Practice shall not of itself render him liable to any criminal or civil proceedings.

**7.4** 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 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) of RIPA and Paragraphs 2.24 to 2.27 of the 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 CSP's itemised billing document to customers (see section 21(4)(b) of RIPA and Paragraphs 2.23 and 2.28 to 2.29 of the 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) of RIPA and Paragraphs 2.30 and 2.31 of the Code of Practice).

**7.5** There are a number of public authorities with statutory power to apply for communications data under Chapter 2 of Part 1 of RIPA. These include:

- Police forces
- NCA

38 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

- HMRC
- Security Service
- SIS
- GCHQ

**7.6** 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.

**7.7** **Annex A** provides tabulated details of the additional public authorities with statutory powers to acquire communications data 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. In 2015, 145 public authorities with statutory powers to acquire communications data used their powers.

**7.8** The following 13 public authorities had their powers to acquire communications data removed in 2015:[39]

- Charity Commission
- Civil Nuclear Constabulary
- Department of Agriculture & Rural Development (Northern Ireland)
- Department for Business Innovation & Skills
- Department for Environment Food, & Rural Affairs
- Department of the Environment Northern Ireland
- Environment Agency
- Food Standards Agency
- The Pensions Regulator
- Port of Dover Police
- Port of Liverpool Police
- Royal Mail Group
- Scottish Environment Protection Agency

**7.9** It is proposed in the IP Bill (schedule 4) that the Food Standards Agency regains powers to acquire communications data for the purpose of preventing and detecting crime or preventing disorder. They have never reported making use of their powers to us. Conversely, public authorities such as the Royal Mail Group made effective use of their powers, right up until they were removed, to investigate and detect criminal offences such as fraud and theft, but they do not appear to regain their powers under the IP Bill.

**7.10** The giving of lawful authority to acquire communications data is set out in the statute and is undertaken by a DP within the public authority acquiring it. Under Chapter 2 of Part 1 of RIPA and the Code of Practice there have to be:

39 SI 2015/228 – The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015

- 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 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 3.18 of the Code of Practice. Except where it is necessary to act urgently, the DP must be independent of the relevant investigation. The DP has to decide whether it is lawful, necessary and proportionate to acquire the communications data to which the application relates.
- a 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 3.19 to 3.30 of the Code of Practice – see in particular the list of functions in Paragraph 3.22. These include:
  - advising both applicants and DPs on the interpretation of Chapter 2 of Part 1 of RIPA, 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.
- 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 2 of Part 1 of RIPA and the Code of Practice.

**7.11** Essentially there are two methods for acquiring communications data – an authorisation under section 22(3) or a notice under section 22(4) of RIPA. 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.

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

**7.13** **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. 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 well-being of the UK 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;
- to assist investigations into alleged miscarriages of justice;
- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident;
- in relation to a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for their death or condition; and
- for the purpose of exercising functions relating to the regulation of the financial services and markets or to financial stability.[40]

**7.14** 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." **Annex A** provides details of the types of data and the statutory purposes under which each public authority can acquire that data.

**7.15** In order to justify that an application is necessary, the application needs, as a minimum, to cover three main points and describe the link between them (see Paragraphs 2.37 and 2.38 of the Code of Practice):

- the event under investigation, such as a crime or vulnerable missing person;
- the person, such as a suspect or witness, and how they are linked to the event, and
- the communications identifier, such as a telephone number or internet protocol address, and how the identifier relates to the person and the event.

**7.16** **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 (see Paragraphs 2.39 to 2.45 of the Code of Practice).

40 SI 2015/228 – The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015. This statutory purpose was added during 2015 so that the Financial Conduct Authority and Prudential Regulation Authority may obtain communications data for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

**7.17** The 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. In order to justify that an application is proportionate the applicant must:

- outline how obtaining the data will benefit the investigation or operation;
- confirm that relevant less intrusive investigations have already been undertaken where possible;
- describe the relevance of any time periods sought and how these are proportionate to the event under investigation;
- consider the rights (particularly to privacy, and in relevant cases, freedom of expression) of the individual and balance these rights against the benefit to the investigation;
- consider any collateral intrusion that may occur; and,
- consider any possible unintended consequences, particularly with regard to complicated requests for traffic data or where the data sought relates to individuals in professions with duties of confidentiality.

## Improved Statistical Requirements

**7.18** In previous reports[41] we have referred to the inadequacy of the statistical requirements in the Code of Practice. In particular the varying systems and administrative practices within public authorities meant the number of applications, authorisations and notices was not necessarily a reliable indicator with which to compare the actual amount of communications data acquired by different public authorities. We have always highlighted that the previous statistical provisions, which required the number of applications and the number of authorisations and notices to be counted, did not give an accurate representation of the amount of communications data actually acquired.

**7.19** A more realistic picture is provided by totalling the number of "items of data" acquired. The relationship between items of data, applications and authorisations and notices was explained in a circular we published in November 2014.[42] We previously made the point that, items of data, as well as being a more accurate representation of the amount of communications data acquired, will also be a considerably larger number than the number of applications, authorisations or notices.

41 See section 7 http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

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

**7.20** As a result of our findings the Home Office sought to improve the statistical requirements and included new provisions in the March 2015 revised Code of Practice. We published guidance[43] in November 2015 to assist public authorities to interpret the new statistical requirements and collate the statistics in a standardised way for the annual return. The new provision for "items of data" has improved transparency by providing a realistic assessment of the use of the powers and enables more accurate comparisons to be drawn between public authorities.

**7.21** The new statistical requirements did not come into force until the end of March 2015 and as a result it was not feasible (technically or practically) for many of the public authorities to apply the new requirements back to the start of January 2015. Understandably it also took a while for some public authorities' technical systems to be configured to capture some of the new requirements. A number of the annual statistical returns have therefore been projected, based on the available information (i.e. three quarters of 2015) to produce a 12-month figure. Evidence shows that the use of these powers remains constant through the year and so we are confident that the projections provide a more accurate picture of use than the previous limited statistical requirements. Other detailed breakdowns are based on partial figures.

**7.22** The rules that apply to each data set are explained further in **Annex B**, along with the number of items of data acquired by each public authority and whether this figure has been projected to equate to 12 months, or not. It is important to note that the counting conventions are completely different to previous years and for this reason it is not possible to draw statistical comparisons with previous reports.

## Statistical Information

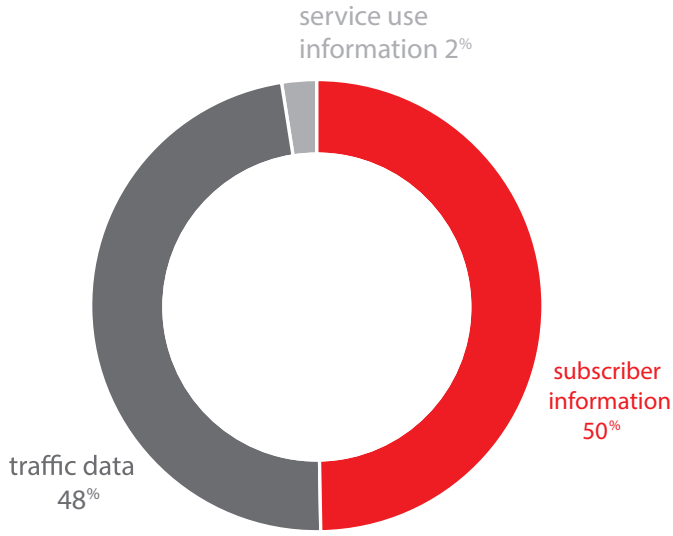
**7.23** **Items of data.** 761,702[44] items of communications data were acquired by public authorities during 2015. An item of data is a request for data on a single identifier or other descriptor, for example, 30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data.

**7.24** **Type of data.** 50% of data acquired was subscriber information, 48% of the data acquired was traffic data and 2% was service use information (**Figure 6**).

43 http://www.iocco-uk.info/docs/SRO%20Circular%20(3)%20Statistical%20Guidance%20Document%20for%20Annual%20Statistical%20Return.pdf

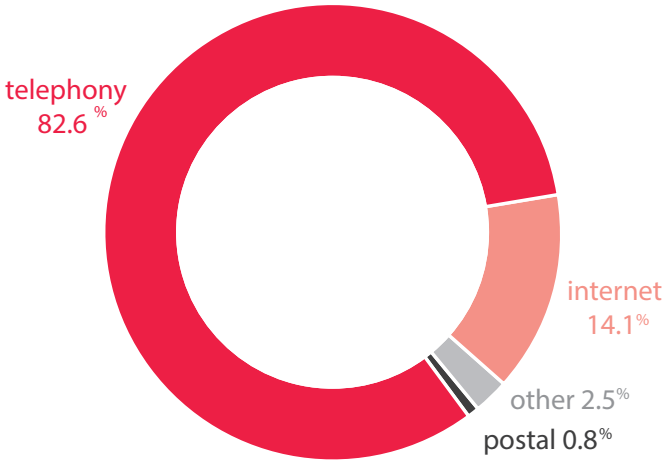
44 Based on projected figures for certain public authorities – see **Annex B**

**Figure 6** *Items of data by type*




**7.25** The majority of items of data (82.6%) related to telephony identifiers e.g. landline or mobile phone numbers, 14.1% related to internet identifiers e.g. email addresses or internet protocol addresses, 0.8% related to postal identifiers e.g. postal addresses and the remaining 2.5% related to "other" identifiers, e.g. bank account or credit card numbers (**Figure 7**).

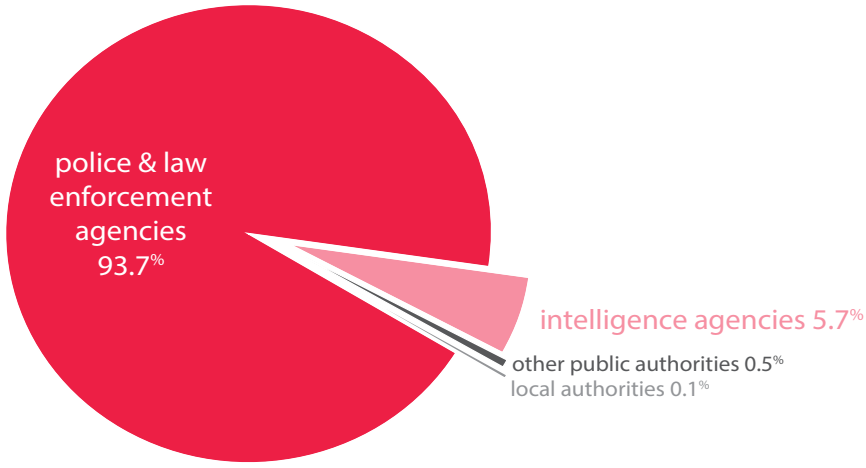
**Figure 7** *Items of data by type of identifier*



**7.26 Public authority usage.** Police forces and law enforcement agencies were responsible for acquiring 93.7% of the items of data, with 5.7% acquired by intelligence agencies, 0.1% by local authorities and the remainder by other public authorities (0.5%) such as regulatory bodies with statutory functions to investigate criminal offences (**Figure 8**).

**7.27 Urgent requests.** Communications data can be acquired in exceptionally urgent circumstances by virtue of an oral application and approval, for example, where there is an immediate threat to life or an urgent operational requirement and there is no time to complete the normal written process (Paragraphs 3.65 to 3.71 of the Code of Practice). Some 11% of the requests in 2015 were orally approved.

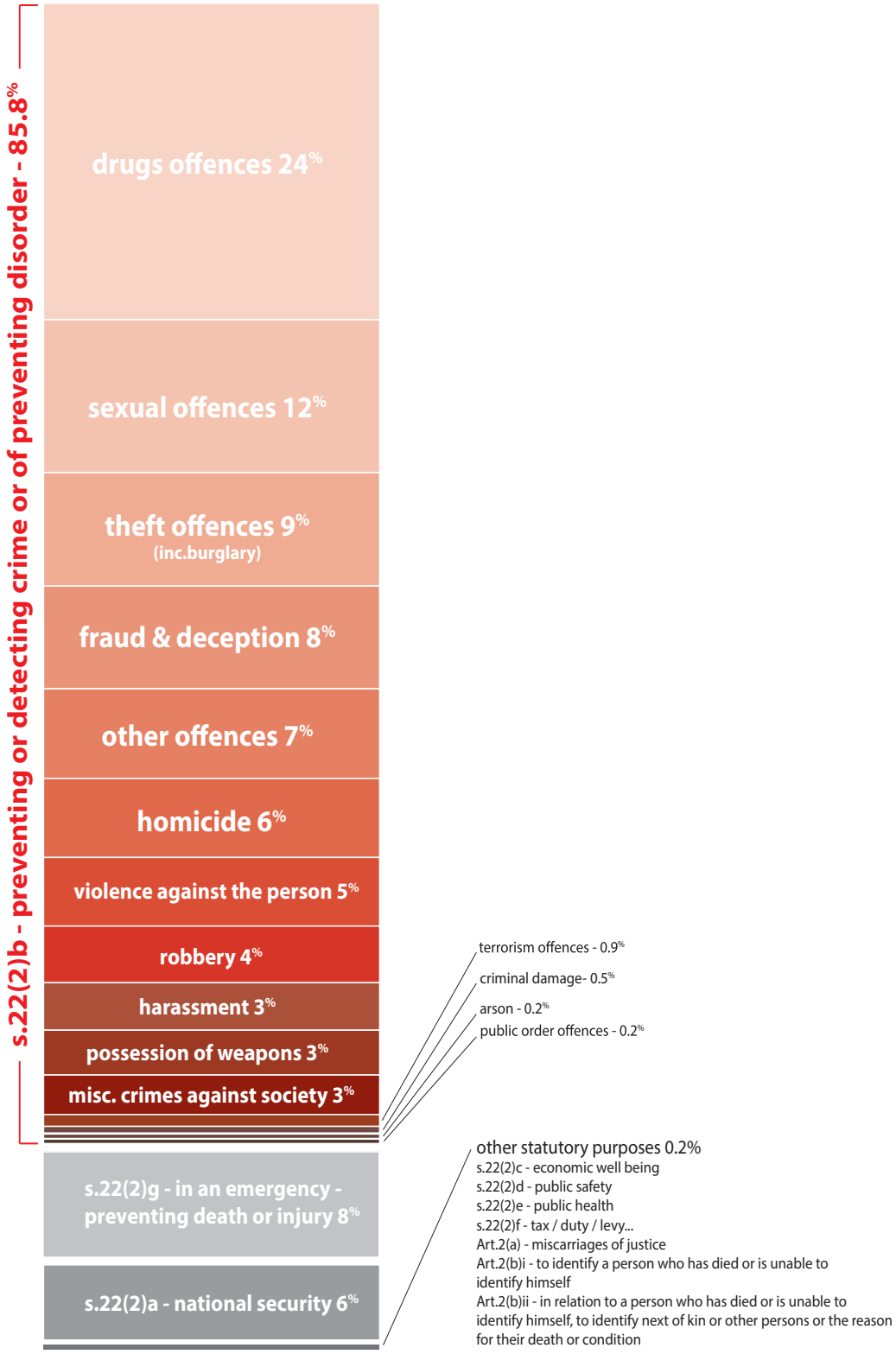
**Figure 8** *Items of data by public authority type*




**7.28 Necessity purpose.** 85.8% of the items of data were acquired for the purpose of preventing or detecting crime or of preventing disorder (section 22(2)(b) of RIPA). 8% was acquired for the purpose 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 (section 22(2)(g) of RIPA) and 6% in the interests of national security (**Figure 9**).

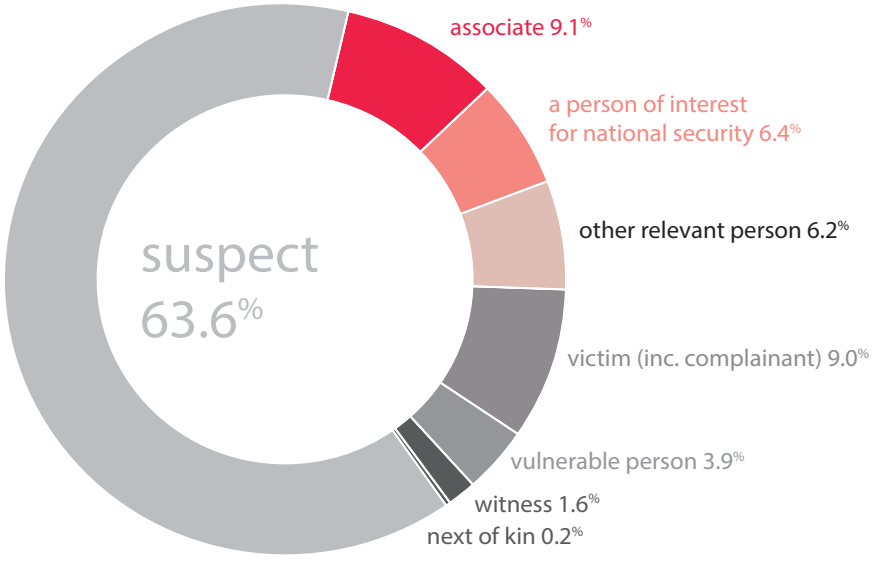
**7.29 Crime type.** **Figure 9** also shows a breakdown by crime type of the items of data acquired for the purpose of preventing or detecting crime or of preventing disorder (section 22(2)(b) of RIPA). 53% of the data was acquired in relation to four crime types: drugs offences, sexual offences, theft offences and fraud and deception offences.

**Figure 9** *Items of data by statutory purpose and breakdown by crime type*



**7.30** **Person type.** Last year we set out a number of compelling reasons why it is not possible for public authorities to report the number of individuals to whom the 761,702 items of data relate to.[45] We made the point that the number of individuals would be much smaller as public authorities make multiple requests for communications data in the course of a single investigation, and also make multiple requests for communications data relating to the same individual. The new statistics require public authorities to record, for each item of data, whether that item relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation. **Figure 10** shows that 70% of requests related to suspects or persons of interest for national security purposes. Approximately 10% of the requests related to victims, complainants or witnesses. For reasons explained in **Annex B**, it is believed that the proportion of data relating to vulnerable persons is under-represented.

**Figure 10** *Items of data by person type*

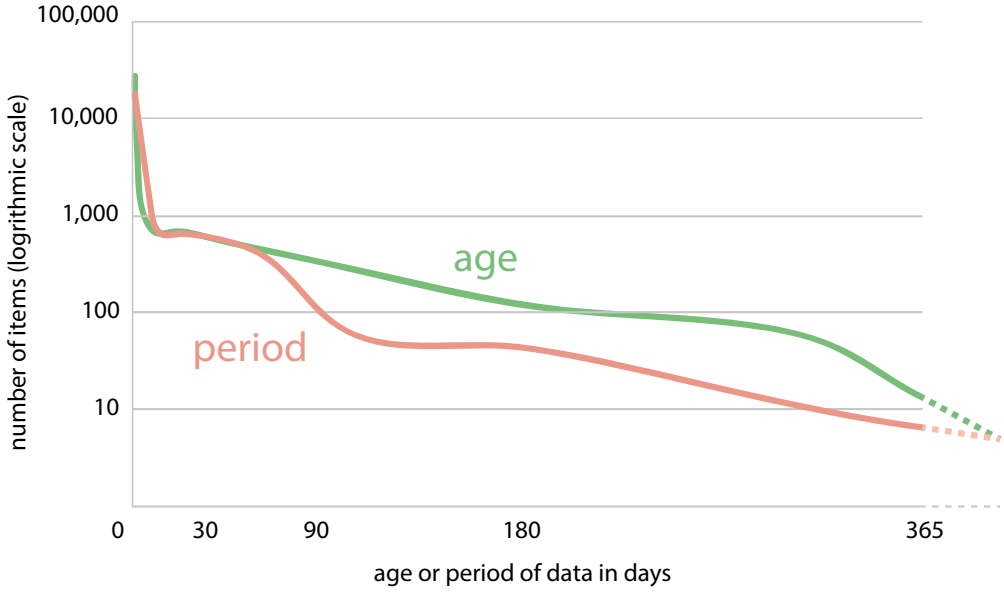



**7.31** **Age of items of data requested.** In terms of the age of the data at the point at which is was acquired, **Figure 11** shows the average trend (in days). This shows that public authorities have a significant demand for current data (i.e. data that is less than one day old), with demand for data falling gradually as its age increases (from a few days old to one year old or over). Approximately 88% of the data requested was for less than four months old at the point of acquisition, 8% was for between four months and one year old, and 5% was for data over 12 months old. This pattern is not necessarily a reflection on the use of older data to an individual investigation. Under DRIPA 2014 the secretary of state can serve a data retention notice on a CSP to retain data for up to 12

45 See Paragraphs 7.29 to 7.31 of our March 2015 report http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

months. Where a CSP has a business need and justification to retain data for longer, they may do so. Generally the amount of data acquired that is older than one year does, to a certain extent, reflect the fact that public authorities do not make applications for data they understand to no longer be retained by a CSP.

**Figure 11** *Items of data by age of the data at the point of acquisition and by period of data requested*




**7.32 Periods of data requested.** **Figure 11** also shows the amount of traffic data or service use information requested. 80% of the requests required data on an identifier for periods of three months or less (for example, one month of incoming and outgoing call data). A high volume of data was acquired for a period of less than one day (approximately 20%) and the vast majority of these would be traffic data requests on internet protocol addresses to determine who was using an internet protocol address at a particular point in time.

**7.33 SPoC & DP scrutiny**. 23% of submitted applications were returned to the applicant by the SPoC for development and a further 6% were declined by the SPoC e.g. where there was a fundamental reason why the application could not be processed such as the unavailability of the requested data. 3% of submitted applications were returned to applicants by DPs for further development and 2% were rejected by DPs (**Figure 12**).

**7.34** **Figure 13** shows a breakdown of the reasons why applications were returned for further development or declined by the SPoC. Almost half were returned for the applicant to provide further justification as to why it was necessary or proportionate to acquire the communications data (49%). Other reasons were the SPoC becoming aware that the data was no longer required or the SPoC identifying errors in the application. Unfortunately a significant proportion of the reasons specified were unclear (e.g. "other", clarity, applicant advised to change).

**Figure 12** *Applications returned for further development or rejected*

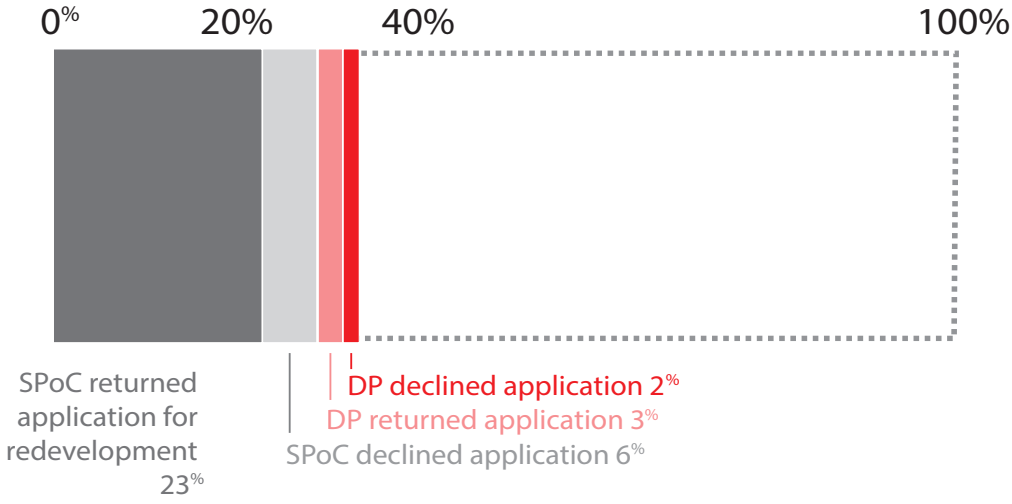
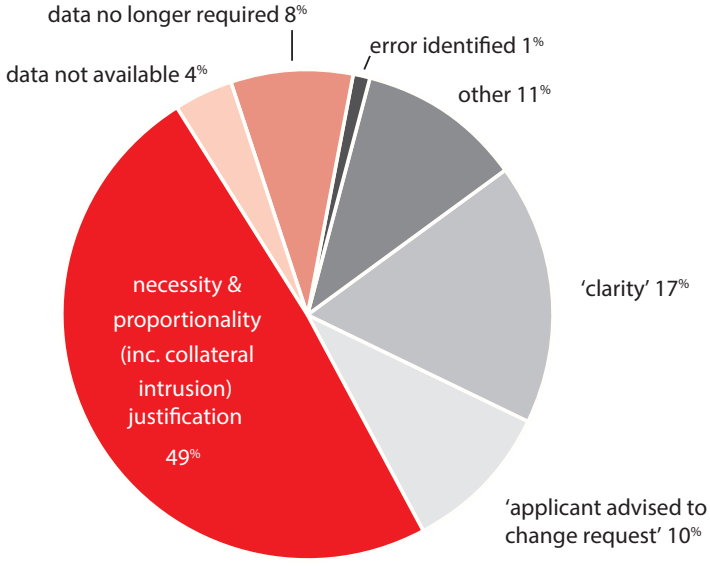
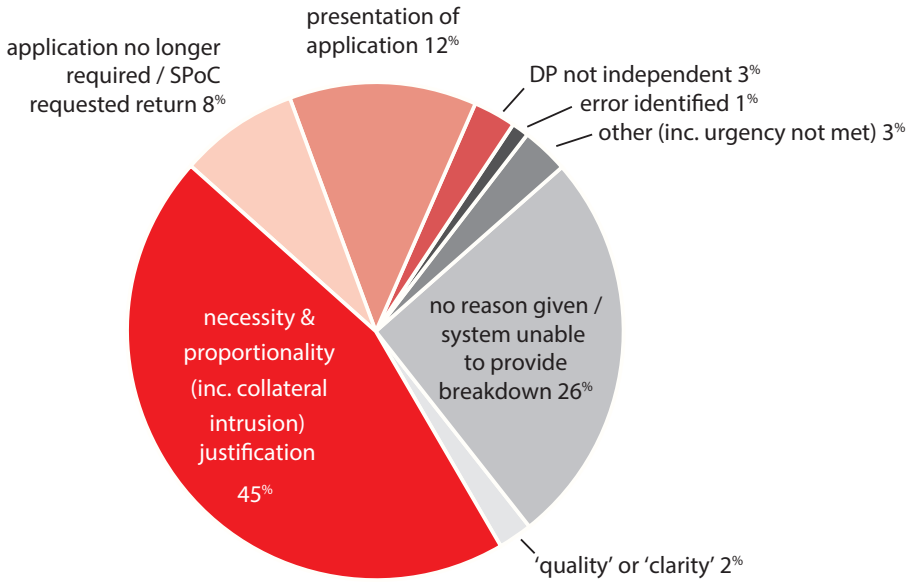



**Figure 13** *Applications returned for further development or declined by a SPoC (by reason)*



**7.35** The main reason for DPs returning or rejecting applications (**Figure 14**) was that the DPs were not satisfied with the necessity and / or proportionality justifications. Some 8% were rejected because the DP had been notified that the data was no longer required, for example, the investigation had progressed in a manner which negated the original reason for acquiring the data, such as a wanted person being located by other means. In 3% of cases the DPs had self-declared that they were not independent of the investigation and asked for the application to be forwarded to another DP to consider who was. Again a significant proportion of the reasons were unclear (e.g. quality or clarity), no reason was given by the DP, or the workflow system was unable to provide a breakdown.

**Figure 14** *Applications returned for further development or declined by a DP (by reason)*




**7.36** It is important for SPoCs and DPs to record sufficiently the reasons for returning applications for further development or declining applications.

**7.37** **Sensitive professions.** The Code of Practice (Paragraphs 3.72 to 3.77) requires applicants and DPs to give special consideration to and take particular care when considering applications for communications data which relate to persons who are members of professions which handle privileged or otherwise confidential information (for example, medical doctors, lawyers etc). In addition public authorities must record the number of such applications and report to the Commissioner annually. Although public authorities have reported their annual figures to us, our examination of those applications highlighted as being related to such professions at the time we inspected some of the public authorities indicates that a large number (potentially as many as 80%) had been miscategorised as relating to a sensitive profession when they did not. Usually this was because the applicant had erroneously stated that the application related to a member of a sensitive profession, rather than there being any ambiguity as to whether the person to which the application related did in fact handle privileged or otherwise

confidential information. We have therefore decided not to publish the statistics in this category as we have serious concerns as to their reliability. We recommend that in future all applications highlighted as relating to sensitive professions are checked by the SPoC and any that have been miscategorised are corrected to ensure accurate reporting. This should be easily achievable as the number of applications of this type per public authority is relatively low.

**7.38** Where we examined the applications that did in fact relate to a member of a sensitive profession, we found that the applications were submitted principally because that individual had been a victim of crime, e.g. a medical doctor, lawyer or MP receiving malicious or threatening communications, or to a much lesser extent because the individual was a suspect in a criminal investigation, both in circumstances related to their occupation e.g. a lawyer suspected of perverting the course of justice, or unrelated to their profession e.g. a medical doctor suspected of committing sexual offences outside the workplace.

## Inspection Regime

**7.39** Our communications data inspections are structured to ensure that key areas derived from Chapter 2 of Part 1 of RIPA 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 meet the requirements of necessity and proportionality;
- query based examination of applications, via 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 were 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.

**7.40** **Number of inspections.** In 2015 IOCCO conducted 72 communications data inspections broken down as follows: 53 police force and law enforcement agency, 3 intelligence agency, 15 'other' public authority inspections and the National Anti-Fraud Network (NAFN) who act as the SPoC for all local authorities. In 2014 we conducted 90 communications data inspections as we were still conducting inspections of individual local authorities. Since December 2014 local authorities have been required to submit their requirements for communications data to the NAFN SPoC and therefore we no longer inspect individual local authorities as we access the records at NAFN. During the NAFN inspection we inspected 71 local authorities who had submitted applications in 2015.

**7.41** 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 three or four days. The inspections of the smaller volume users are conducted by one inspector and generally last one day.

**7.42** **Samples**. It is important that IOCCO scrutinises a sufficient sample of the individual applications, but 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."*[46] In the smaller public authorities it is usually feasible for the inspectors to examine all of the applications submitted in the period being examined. For the larger volume users sampling must be undertaken. IOCCO conduct two types of sampling, random sampling where the application process is examined from start to end, and query based examinations where key parts of the process are scrutinised.

**7.43** In 2015 IOCCO inspectors scrutinised at random approximately 15,000 applications during the 72 inspections and over 117,000 applications were subject to query based examinations.

**7.44** 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,

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

although random sampling may only detect one 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.

**7.45 Query based examinations.**[47] We engage directly 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 approximately 90% of the communications data requests). The software companies have developed capabilities to enable IOCCO to retrieve data by means of query based examinations 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 information 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.

**7.46** We are able to examine, within the operational environment, the interference actually being undertaken. In a scientific sense, we test the operational hypothesis set down in the initial application that was authorised. 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 or breaches resulted from the interference or intrusion.

47 Query based examinations involve searches against defined criteria or subjects.

**7.47** **Inspection Reports.** The reports contain a review of compliance against a strict set of baselines that derive from Chapter 2 of Part 1 of RIPA 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

**7.48** The total number of recommendations made during our 72 communications data inspections in 2015 was 366 (**Figure 15**). 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 or non-compliance with Chapter 2 of Part 1 of RIPA 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.

**7.49** This year of 29 recommendations (8%) were red, 203 (55%) amber and 134 (37%) green. Comparisons with previous years are difficult because the public authorities being inspected are not the same and the number of inspections conducted each year differs. However, whilst the proportion of red, amber and green recommendations has remained broadly consistent over the past four years, the average number of recommendations per inspection in 2015 rose from approximately four to five per public authority (**Figure 15**). Analysis shows that the increase stems from compliance issues relating to new provisions in the Code of Practice i.e. those concerning record-keeping (statistical) requirements, DP independence and applications relating to sensitive professions, which are discussed in more detail below.[48]

**7.50** 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 complied with following the previous inspection. While it is difficult to compare previous years because the public authorities inspected each year change, it is possible to gauge whether compliance is improving or not by comparing a public authority's rating in 2015 to the rating from its previous inspection. 51 of 72 the public authorities inspected maintained their overall rating (49 good & 2 satisfactory). 8 public authorities raised their overall level of compliance rating (6 from satisfactory to good, 1 from poor to satisfactory and

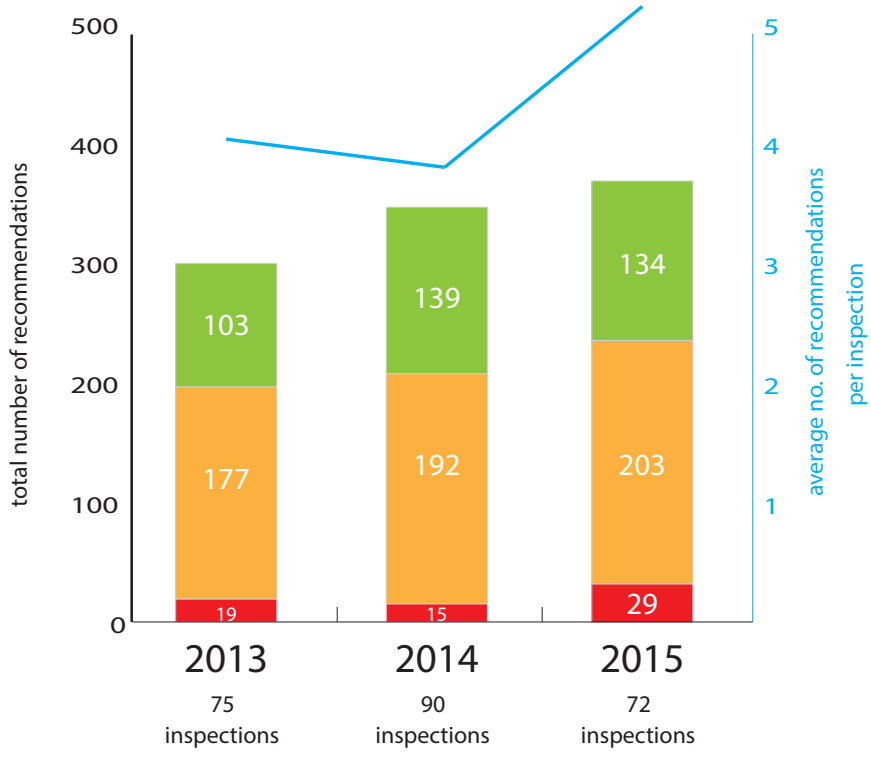
48 Just over one quarter of the 366 recommendations made in 2015 related to new provisions in the Code of Practice. Without them the average number of recommendations per inspection would be almost identical to the 2014 average.

1 from poor to good). In 13 public authorities the rating dropped (10 from good to satisfactory, 1 from good to poor & 2 from satisfactory to poor).

**7.51** Over two thirds of the 366 recommendations fell into seven principal categories:

- Quality of applications
- Record keeping
- DP independence
- DP considerations
- SPoC efficiency and effectiveness
- Sensitive professions
- Errors

**Figure 15** *Total Red, Amber & Green recommendations from communications data inspections 2013-2015*




**7.52** **Quality of applications (52 recommendations)**. During our inspections we identified applications which did not sufficiently justify why it was necessary and / or proportionate to acquire the communications data, in particular cases where:

- the applicant did not make clear how the communications identifier was linked to an enquiry;
- the wrong statutory necessity purpose had been specified in the application,

for example, section 22(2)(d) in the interests of public safety or section 22(2)(e) for the purpose of protecting public health when the requirement related to the prevention or detection of crime;

- the relevance of the date or time periods sought had not been justified.

**7.53 Record-keeping (44 recommendations).** We found that in a number of cases the record-keeping requirements in Paragraphs 6.1 to 6.8 of the Code of Practice (including a number of the revised statistical requirements) were not complied with, specifically:

- applications under section 22(2)(b) were being incorrectly categorized by crime type - either the list of offences did not align properly to statutory offences or to the Home Office's recorded crime list or, the list was being applied inconsistently by applicants.
- the procedures in place for applications processed outside the main workflow system, e.g. by specialist departments or those approved orally, had not been amended to meet the revised statistical requirements.

**7.54 DP independence (34 recommendations).** Paragraph 3.12 of the Code of Practice states that DPs ***must*** be independent from operations and investigations when granting authorisations, or giving notices related to those operations. This is a strengthening of the previous Code of Practice which stated that DPs ***should*** not be responsible for granting authorisations or giving notices in relation to investigations in which they are directly involved.

**7.55** This policy change in March 2015 was brought about in response to the European Court of Justice (ECJ) Judgement which struck down the Data Retention Directive (2006/24/EC) on the grounds the Directive did not include sufficient safeguards as to why and by whom such data may be accessed. The Judgment did not prevent Member States implementing their own laws requiring the retention of communications data but it did critically note that the Directive itself contained no safeguards for access to the retained data, including in relation to the independence of the person authorising access to the retained data.

**7.56** In our July 2015 report we set out that we were concerned that SPoCs within public authorities seemed to be unaware of the detail of the policy changes in the March 2015 Code of Practice. The period allowed by the Government for the drafting, consultation and implementation of the Code of Practice was ambitious, and with hindsight, more extensive consultation with key stakeholders and more time for all to consider the issues properly would have enabled some of the provisions to be better refined to make certain matters clearer. It would also have ensured that all public authorities were aware of the changes and had time to consider the operational implications.

**7.57** We received a number of questions from public authorities regarding the change in policy around DP independence and its operational consequences. On 1 June 2015 we published a circular to SROs to provide clarification about the new provisions and to assist public authorities to implement procedures to comply. This was a significant change for a number of the larger public authorities (such as police forces, intelligence agencies

and law enforcement agencies) to implement. It is understandable that a number of those public authorities took some months to implement the new requirement because it required significant organisational, policy and IT system changes.

**7.58** Unsurprisingly during our inspections in 2015 we identified a number of compliance issues or concerns in relation to this area of the process. The compliance issues or concerns broadly fell into four categories:

1 Those public authorities where instances of non-compliance were identified during inspections or were reported to us (i.e. DPs had considered and approved applications when they were not independent of the investigations or operations to which the applications related). 7 public authorities fell into this category;

2 Those public authorities where we could not be satisfied that the systems and procedures were sufficient to ensure compliance with the independence requirements but we found no individual instances of non-compliance. In some cases no clear strategy had been implemented by the public authority, or we questioned the reliance on DPs self-certifying their independence, particularly where they were considering applications from departments or areas for which they had strategic accountability. 14 public authorities fell into this category;

3 Those public authorities where we were satisfied that the procedures were sufficient overall, but where recommendations were made to enhance the safeguards further to ensure that independence was always achieved (e.g. improved auditing capabilities to check a DP is independent or formalising arrangements for applications to be considered in the absence of the principal DP). 8 public authorities fell into this category;

4 Those public authorities who are not able to call upon the services of a DP who is independent from the investigation or operation, but who had not notified us of this fact in accordance with Paragraph 3.13 of the Code of Practice. 4 "other" public authorities fell into this category and we separately prompted NAFN to audit the local authorities registered to use their SPoC services. NAFN reported to us that 49 of the 228 local authorities registered with them were not able to call upon the services of an independent DP, but only approximately half of the 49 local authorities used their powers in 2015. The reasons for being unable to call upon an independent DP were twofold. First, applications emanated from small specialist criminal investigation departments within public authorities who are not law enforcement or intelligence agencies (such as local authorities). Secondly, a number of the public authorities are restricted in the number of individuals who can act as a DP because the relevant statutory instrument prescribes a job title or position which only one individual holds within the organisation and, by the very nature of that role, they would not be entirely independent. In the case of local authorities it is important to note that although the DP might not be independent, local authorities cannot acquire communications data without the authorisation first being approved by a relevant judicial authority.[49]

49 See Section 37 of the Protection of Freedoms Act 2012 - "Relevant judicial authority" means—

**7.59** In relation to the 24 public authorities in categories 1, 2 and 3 above, all but one has confirmed to us that they have implemented the necessary procedures to ensure independence. We have inspected a number of those public authorities since and have confirmed that their procedures are effective to ensure independence. We will continue to scrutinise this area closely on future inspections. The Security Service is the only public authority that has still not implemented measures to ensure DP independence.

**7.60** **DP Considerations (26 recommendations).** We identified during inspections that a number of DPs were recording short and / or formulaic written considerations when approving applications. Good practice recommendations were given to those public authorities to assist the DPs to improve the quality of their considerations and provide sound evidence that they had considered each application individually.

**7.61** **SPoC efficiency and effectiveness (51 recommendations).** A broad range of recommendations were made in this area. Some were concerned with ensuring that the SPoC provides a robust guardian and gatekeeper function e.g. by being sufficiently resourced, by providing better quality advice to applicants or DPs about the proposed collection strategy or conduct to be undertaken. Other recommendations were designed to improve efficiency e.g. more dynamic management of any application clarifications, amendments or refinements to improve the efficiency of the process.

**7.62** **Sensitive professions (27 recommendations).** On 6 October 2014, following national concerns relating to the protection of journalistic sources, we launched an inquiry into the use by police forces of powers under Chapter 2 of Part 1 of RIPA to identify or determine journalistic sources. Our inquiry report[50] was published in February 2015 and recommended that such applications should be approved by a judge. The Prime Minister committed to implement the recommendations as soon as possible and the Serious Crime Act, which received Royal Assent on 3 March 2015, amended section 71 of RIPA to require the Code of Practice to include provision designed to protect the public interest in the confidentiality of journalistic sources. On 25 March 2015 the revised Code of Practice came into force requiring all UK law enforcement agencies to seek judicial authorisation when applying for communications data to identify or determine journalistic sources.

**7.63** Regrettably we identified four investigations where data had been acquired to identify or determine journalistic sources after the Code of Practice came into force on 25 March 2015 without seeking judicial approval. In some of these cases the conduct took place on the day after the Code of Practice came into force or shortly thereafter. In all but one of these cases the Commissioner determined that although the conduct was serious it was not wilful or reckless and it did not adversely affect any individual significantly. The one case in which the Commissioner gave a determination that the conduct was reckless, in line with his power under Paragraph 8.3 of the Code of Practice, related to Police

(a)in relation to England and Wales, a justice of the peace,
(b)in relation to Scotland, a sheriff, and
(c)in relation to Northern Ireland, a district judge (magistrates' courts) in Northern Ireland,

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

Scotland and has been widely publicised.[51] In this instance the Commissioner informed four individuals about the conduct and provided them with sufficient information to engage the IPT. All have subsequently made valid complaints and Police Scotland have conceded to the IPT that the communications data authorisations were obtained unlawfully. A hearing is scheduled in July 2016 to decide outstanding points of law and to consider a remedy.

**7.64** In our July 2015 report we commented on the speed at which the Code of Practice provisions concerning journalistic sources came into force, the lack of stakeholder engagement around the change and the fact that many public authorities were not even aware that the Code of Practice had come into force until some time afterwards. There is also a lack of clarity concerning the provisions in the Code of Practice which should be addressed by the Home Office, for example:

- why is the judicial provision limited to law enforcement agencies?
- what authorisation route do public authorities who do not have powers under PACE use for such applications?
- the interchange of the words "identify" and "determine" in Paragraphs 3.78 to 3.84 of the Code of Practice has caused misunderstanding.
- when acquiring data on a journalist's phone because, for example, they are the victim of an offence or because it is necessary and proportionate to identify or determine their source, the consequence of acquiring that data is arguably the same even though in the former case that consequence might be unintended (i.e. there is a likelihood that confidential journalistic sources may be identified). In the latter case judicial approval is required, but in the former it is not. The infringement of Article 10 ECHR rights is the same irrespective of the intention of the applicant if the data acquired can be used to determine a journalistic source. A lack of unity in the language of the Code of Practice creates opportunities for different interpretations. This could lead to circumstances where two applications facing exactly the same investigative issues adopt different approaches.

**7.65** The Code of Practice (Paragraphs 3.72 to 3.77) also requires applicants and DPs to give special consideration to and take particular care when considering applications for communications data which relate to persons who are members of professions which handle privileged or otherwise confidential information (e.g. medical doctors, lawyers etc) are undertaken.

**7.66** In 2015 the inspectors identified instances in 13 public authorities where applications of this nature contained insufficient consideration of the degree of interference with an individual's rights and freedoms. In these cases we sought further information from the applicant, investigator and / or DP and were satisfied that although the application failed to articulate properly these considerations, they had in fact been

51 http://www.iocco-uk.info/docs/Memorandum%20of%20Commissioner's%20Determination%20(Redacted).pdf

duly considered and the requests were necessary and proportionate. We have already made the point that the majority of these applications were submitted principally because that individual had been a victim of an crime, e.g. a medical doctor, lawyer or MP receiving malicious or threatening communications.

**7.67** We have already made the point in our July 2015 report that the speed at which the legislative changes were enacted and the resultant unrefined elements of the Code of Practice has left us having to provide much needed clarity on Government policy rather than simply auditing against it. We welcome the fact that public authorities come to us for guidance in this area and will continue to be as helpful as possible, but make the point that it is crucial for public authorities to also seek clarity from the Home Office to ensure that the Home Office is aware of the policy issues and can seek to resolve them in future legislation.

**7.68** **Errors (16 recommendations).** Following our review of serious errors in our July 2015 report a greater number of recommendations have been made for public authorities to implement measures to reduce error instances, particularly where errors can have serious consequences e.g. those which relate to internet protocol resolutions. The inspectors also found, as was the case in previous years, instances where erroneously acquired data of no relevance to an investigation had not been destroyed after the error report was made to IOCCO as required by the Code of Practice. Communications Data errors are considered in further detail later in this report.

## Inquiries into Specific Issues

**7.69** **Journalistic source inquiry.** We published our inquiry report[52] in February 2015 and that report led to the Code of Practice amendments which we have previously discussed in this report.

**7.70** **Section 94 of the Telecommunications Act 1984.** In October 2015 IOCCO started its review of directions issued under section 94 of the Telecommunications Act 1984. Our review report was published on 7 July 2016.[53]

**7.71** **Institutional overuse.** Our March 2015 report[54] set out the findings of our inquiry into whether there was significant institutional overuse of communications data powers by police forces and law enforcement agencies. We concluded there was not but we did find that a proportion of the applications did not adequately deal with the requirements of necessity and proportionality and we found some examples where the powers had been used improperly or where they had been used unnecessarily. We said that we would

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

53 http://iocco-uk.info/docs/56208%20HC33%20WEB.pdf

54 See Paragraphs 7.59 to 7.68 http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

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.

**7.72** This year we decided to conduct a comparative study of investigations where communications data has or 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. We chose to examine the communications data strategies and operational actions for robbery investigations.

**7.73** During each police force inspection we sought to examine all reported robberies for a specific month and any associated applications for communications data. The number of robberies reported for a specific month varied considerably between the different police forces, from hundreds in some urban force areas to a handful in some of the more rural forces, to the extent that it was necessary to widen the period examined in certain forces to evaluate a reasonable sample.

**7.74** We found that the proportion of applications submitted in relation to reported robberies varied significantly between police forces. Typically the police force would seek to acquire data where a communications device (e.g. mobile phone) had been stolen or where a suspect had been identified and there was a need to establish that person's movements (e.g. to test an alibi). In the majority of robbery offences no mobile phone had been stolen. Sometimes if a mobile phone had been stolen it was blocked on the National Mobile Property Register (NMPR).[55] In such cases no communications data was acquired because there was sufficient evidence available from other sources to charge a suspect, or alternatively there was good reason to question the credibility of the robbery report. Conversely, in a small number of cases examined by the inspectors it appeared from the crime report or other information available that the acquisition of communications data may well have been a possible line of enquiry that had not been considered or pursued. Overall the inspectors concluded that communications data was being acquired proportionately in relation to robbery investigations and there was no automatic recourse by police forces to acquiring communications data.

**7.75** Whilst our inquiry into institutional overuse of communications data has now concluded the inspectors maintain their vigilance to disproportionate acquisition by public authorities by continuing to examine at each public authority the proportionality of the totalilty of the communications data acquired in connection with large-scale investigations, and acquisition relating to other specific crime types (e.g. road traffic offences, malicious communications etc.).

55 https://thenmpr.com/

# Communications Data Errors

### What is a communications data error?

**7.76** Paragraphs 6.11 to 6.28 of the Code of Practice explain the point at which errors occur and the actions required of the public authority or the CSP.

**7.77** An error occurs when a DP has granted an authorisation and the acquisition of data has been initiated; or has given notice and the notice has been served on a CSP.

**7.78** There are two categories of errors: reportable and recordable.

**7.79** **Recordable errors:** 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. For example, where human error, such as the transposition of digits occurs, but does not result in the wrongful acquisition or disclosure of communications data. The record will explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. During our inspections we examine the recordable errors along with any steps the public authority has taken to prevent recurrence.

**7.80** **Reportable errors:** In cases where an error has occurred that has led to communications data being acquired or disclosed wrongly a reportable error will arise. For example, where the wrong type of data or data in relation to the wrong telephone number is acquired or disclosed. In some instances wrongful disclosures infringe the rights and freedoms of individuals not connected with the particular investigation or operation. Reportable errors must be reported to IOCCO in no more than five working days of being discovered (see Paragraphs 6.15 and 6.19 of the Code of Practice). The error report must explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and, provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur.

**7.81** The vast majority of reportable errors are self-reported to us by public authorities and CSPs. As mentioned in our July 2015 report there is a strong culture of self-reporting when things go wrong by both public authorities and CSPs.

**7.82** We recently devised new error report form templates to be used by public authorities[56] and CSPs[57] to improve the quality of the information provided in the reports, in particular to tease out sufficient detail to reveal the root cause of any error, the impact that error has had, the measures implemented to prevent recurrence and to confirm that any data that has been acquired erroneously has been destroyed.

56 http://www.iocco-uk.info/docs/Public%20Authority%20Error%20Report%20Form%20vJun16.docx

57 http://www.iocco-uk.info/docs/CSP%20Error%20Report%20Form%20vJun16.docx

## Error Statistics

**7.83** In terms of how errors are counted, one erroneous human act will typically correspond to one erroneous disclosure (e.g. an applicant submits a request for subscriber information on the wrong telephone number and erroneous subscriber details are acquired). When however the erroneous act relates to a technical system, for example a CSP's secure disclosure system (more on such systems later), one error is likely to have multiple consequences and to result in a larger number of erroneous disclosures.

**7.84** The total number of errors reported to us in 2015 was 1199. This is an increase of 20% on the 998 errors reported in 2014. As the majority of errors are self-reported it is difficult to comment whether this represents greater vigilance in the spotting of errors; less care being taken; or is proportionate to the type of data being acquired. A comparison with the 2014 figures reveals that the main cause for the overall rise is a larger number of incorrect communications identifiers being submitted by applicants and SPoCs or data being acquired over the incorrect date or time period.

**7.85** It is of note that a large proportion of these errors (including the majority of errors where applicants specified the incorrect date or time) relate to internet protocol addresses. This is significant considering internet protocol addresses account for less than 14% of the items of data acquired by public authorities and given the potential for serious consequences to result from mistakes that are made when resolving internet protocol addresses. For example, an internet protocol address is often the only line of inquiry in a child protection case (so called single strand intelligence), and it may be difficult for the police to corroborate the information further before taking action. Any police action taken erroneously in such cases, such as the search of an individual's house that is unconnected to the investigation or a delayed welfare check on an individual whose life is believed to be at risk can have a devastating impact on the individuals concerned.

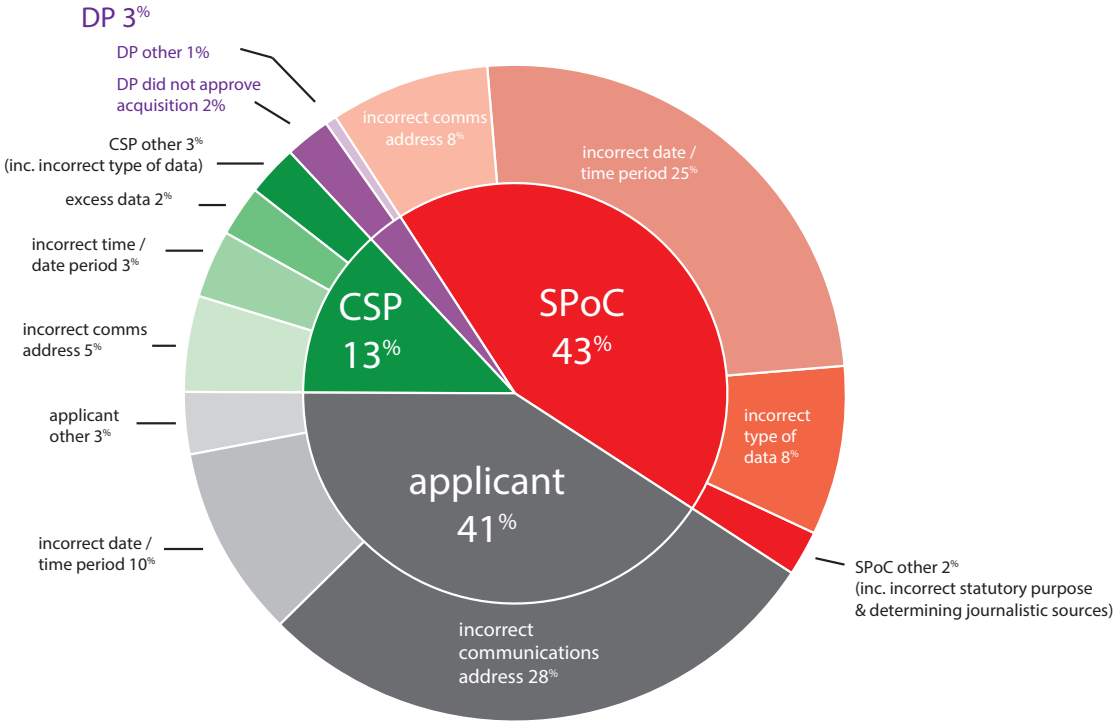
**7.86** We highlighted the vulnerability of resolving internet protocol addresses in our July 2015 report[58] and, to summarise, the fact that internet protocol addresses are generally dynamic in nature and public authorities receive information about internet protocol addresses linked to crimes (and other statutory purposes) in numerous time zones and date formats, and are correspondingly required to acquire data from CSPs in numerous time zone and date formats to resolve which individual they relate to, presents opportunities for errors to occur.

**7.87** It is expected that the need for public authorities to resolve internet protocol addresses will only increase over time and it is therefore crucial that public authorities work closely with CSPs and other system providers to implement both technical solutions and pre and post acquisition checks to prevent such errors. or ensure they are promptly identified. We have seen examples within a number of public authorities where the implementation of such measures, including those which we recommended in our July 2015 report, have prevented erroneous data from been acquired in the first place, or

58 http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf

have led to the identification of erroneous results averting serious consequences. Indeed the post acquisition verification measures that a number of SPoCs have introduced may in fact be partially responsible for the increase in errors reported to us.

**Figure 16** *2015 Errors breakdown by cause*




**7.88** **Figure 16** shows the breakdown of the 1199 errors by responsible party and cause. 84% of errors were caused by applicants or SPoCs, 13% by CSPs and 3% by DPs.

**7.89** Every error report received by IOCCO is assessed to determine the level of impact upon an individual or investigation and whether the error instance may have the potential to affect disclosures made to other public authorities or require changes to be made to systems and procedures to prevent recurrence.

## Serious Error Investigations

**7.90** In our July 2015 report[59] we sought to explain why the in-depth error investigations that we conducted in 2014 constituted "serious errors."

**7.91** Paragraph 6.22 of the Code of Practice came into force in March 2015 and

59 http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf

introduced a discretionary power for the Commissioner to investigate reportable errors deemed to be of a "serious nature". In such cases the Commissioner *may* investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner *may* inform the affected individual, who may make a complaint to the IPT. There is no definition of what circumstances might constitute errors of a "serious nature."

**7.92** We have considered the implication of this discretionary power and its interrelationship with the Commissioner's mandatory power in Paragraph 8.3 of the Code of Practice to inform any individual who has been adversely affected by a person within a public authority wilfully or recklessly using RIPA powers to acquire communications data. "Wilful and reckless failures" are also undefined in the Code of Practice as is the term "adversely affected".

**7.93** The Commissioner has determined that a "wilful" failure may arise for the purposes of Paragraph 8.3 of the Code of Practice when any person within a relevant public authority intentionally and deliberately acts in manner inconsistent with their powers or duties under RIPA and there has been an adverse impact on an individual. They may act "recklessly" for the purposes of Paragraph 8.3 when exercising their powers, if they failed take account of an obvious and serious risk and there was adverse impact on an individual.

**7.94** In an attempt to provide some clarity and guidance to public authorities on the provisions in the Code of Practice, the circumstances in which we may classify an error as "serious" include:

1 Technical errors relating to CSP secure disclosure systems which result in a significant number of erroneous disclosures.

2 Errors where the public authority has, as a consequence of the data, initiated a course of action that impacts on any individual (for example, the sharing of information with another public authority stating a person is suspected of a crime, an individual being visited or the execution of a search warrant at premises or the arrest of a person).

3 Errors which result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

**7.95** We carry out in-depth and detailed investigations into any errors classified as serious to determine fully the circumstances and impact. In some cases there may be no adverse impact on any individual (e.g. a technical system error which led to false negative results) and we would just investigate the cause of the error and ensure measures are put in place to prevent recurrence. In cases where there was wilful or reckless conduct and an individual had been adversely affected the Commissioner would invoke his power under Paragraph 8.3 and inform the individual concerned. In cases where there was no wilful or reckless conduct, the Commissioner would consider using his discretionary power in Paragraph 6.22 i.e. if the error was deemed to be of a "serious nature" the Commissioner would assess the impact of the interference on the affected individual's rights and may decide to inform the individual of the error.

**7.96** We note that the IP Bill (clause 207) has brought some further clarity to this area by introducing a "significant prejudice or harm" threshold as well as a public interest test. However in accordance with the above considerations, we have already set out in various publications, including in **Section 5** of this report, some of the practical difficulties that the Investigatory Powers Commissioner may encounter when operating the powers as currently drafted.

**7.97** During 2015 we undertook 34 serious error investigations. We concluded that in 11 of the 34 cases the errors did not in the end meet our serious error criteria.

**7.98** Of the remaining 23 cases, 14 of the serious errors were human errors and 9 were system errors.

**7.99** The impact or consequences of 14 human errors were as follows:

- persons unconnected to an investigation were visited by police (5);
- a delayed welfare check on a vulnerable person (6);
- a search warrant was executed at an address of a person unconnected to the investigation and / or persons unconnected to the investigation arrested (3).

**7.100** Where a technical system error occurs it can have multiple consequences and is likely to result in a large number of erroneous disclosures. The 9 technical system errors resulted in 2036 erroneous disclosures. In the vast majority of these cases the error was quickly identified and the erroneous data was destroyed without any action being taken upon it. 2 of the 9 technical system errors led to 14 instances where search warrants were executed at the addresses of persons unconnected to the investigation and / or persons unconnected to the investigations were arrested, 1 instance where a person unconnected to the investigation was visited by police, and 1 instance where the erroneous data resulted in a delayed welfare check on a vulnerable person.

**7.101** One of the 23 cases was discovered during an inspection of a police force. As a result of a detailed investigation into the circumstances of this case the Commissioner determined that two applications submitted in relation to that investigation were not necessary or proportionate for the stated purpose (the prevention and detection of crime). The Commissioner determined that the individual to whom the applications related had been adversely affected because they were visited by police in connection with that investigation. In accordance with Paragraph 6.22 of the Code of Practice the Commissioner informed the individual of the error and provided sufficient information for them to pursue a complaint with the IPT. The individual concerned has decided not to pursue the matter further and to respect the privacy of that individual we do not intend to provide any further information on the matter.

# Points of Note

### Communications Data

761,702 items of communications data were acquired during 2015. 48% of the items of communications data were traffic data, 2% service use information and 50% subscriber information.

145 public authorities acquired data in 2015. 93.7% of the applications for communications data were made by police forces and law enforcement agencies, 5.7% by the intelligence agencies and 0.6% by local authorities and other public authorities (regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions).

In 2015 IOCCO conducted 72 communications data inspections. We scrutinised at random approximately 15,000 applications and in addition over 117,000 applications were subject to query based examinations.

366 recommendations emanated from our inspections, an average of 5 recommendations for each public authority.

1199 errors were reported to IOCCO in 2015, an increase of 20% from the previous year. The main causes for the overall rise are a larger number of incorrect identifiers being submitted by applicants on their applications or, both applicants and SPoCs acquiring data over the incorrect date or time period. Once again we highlight that a significant number of these errors relate to Internet Protocol addresses being incorrectly resolved to subscribers, which can have serious consequences.

23 serious errors were investigated in 2015 (9 technical system errors and 14 human errors). The 9 technical system errors resulted in multiple consequences and a large number of erroneous disclosures (2036). The consequences of the 23 serious errors were as follows: 17 instances where search warrants were executed at the addresses of persons unconnected to the investigation and / or persons unconnected to the investigations arrested, 6 instances where persons unconnected to the investigations were visited by police, 7 resulted in delayed welfare checks on vulnerable persons and in the remaining cases there was no significant impact as typically the error was identified prior to the information being acted upon.

Regrettably IOCCO identified four investigations where data had been acquired to identify or determine journalistic sources without judicial authorisation. In one case the Commissioner determined that the conduct was reckless and informed the affected individuals who subsequently made complaints to the Investigatory Powers Tribunal (IPT). In a separate case the Commissioner invoked his discretionary power under Paragraph 6.22 of the Code of Practice. In this case he determined that two applications were not necessary or proportionate and he informed the individual who had been adversely affected by the conduct.

# Section 8

## Investigation of Electronic Data Protected by Encryption

**8.1** Part 3 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.

**8.2** The requirements of Part 3 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) of RIPA). The measures in Part 3 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 and encryption).

**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 3 of RIPA. No public authority may serve any notice under section 49 of RIPA 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 3: the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner.

**8.5** IOCCO's responsibilities under Part 3 of RIPA 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 3, particularly the grant of appropriate permission for the giving of a section 49 notice in relation to information obtained under Part 1 (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 1.

**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 3 of RIPA, 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. We can confirm that in 2015 no section 49 notices were issued by any secretary of state in relation to information obtained under Part 1 of RIPA (i.e. intercepted material and other related communications data).

# Section 9
## Complaints of unintentional electronic interception

**9.1** The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interception) Regulations 2011 ("the Regulations") made amendments to Part I RIPA 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 UK had failed to adequately transpose European Union (EU) law requirements concerning the confidentiality of electronic communications, specifically in relation to the interception of communications.[60]

**9.2** RIPA 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[61], without a warrant. The changes to RIPA, brought about by the Regulations, relate to interception without a warrant.

**9.3** RIPA provides that CSPs may lawfully and legitimately intercept communications when it is necessary for them to do so for specified purposes (for example, to manage their networks).[62] Where businesses choose to carry out interception to provide value-added services, an activity which is carried out at the discretion of CSPs, RIPA requires the consent of both the sender and the recipient of the communications that will be intercepted.[63] It also provides for a criminal sanction against intentional interception of communications without lawful authority, thus providing additional protection for an individual'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, a civil sanction was created for the unlawful interception of electronic communications where the interception does not meet the standard of intent required in the criminal offence. Secondly, 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.

**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 the Commissioner if he is satisfied that certain communications have been intercepted without lawful authority at any place in the UK. In addition, the Commissioner will need to be satisfied 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.

60 In particular, the E-Privacy Directive and the now defunct Data Protection Directive

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

62 See section 3(3) of RIPA

63 See section 3(1) of RIPA

**9.6** The Regulations (and therefore the Commissioner's responsibilities under them) came into effect from 16 June 2011. We have previously published guidance[64] in accordance with the Regulations. The guidance provides information on the circumstances in which the Commissioner will consider it appropriate to issue a monetary penalty notice, how he will determine the amount of the penalty and the mechanism for handling complaints. If a person has reasonable cause to believe their consent relating to the interception of their communications was not obtained during the provision of such a service they may seek to make a complaint to the Commissioner under the Regulations. The complaints process is not the appropriate channel through which adverse comments about the way CSPs, based within the UK and elsewhere, conduct their business.

**9.7** In 2015 we received a number of complaints from members of the public, but determined that all related to conduct alleged to have been undertaken by public authorities. We advised those individuals to make a complaint to the IPT which has exclusive jurisdiction in the UK to hear such complaints.

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

# Section 10
# Prisons

**10.1** This section provides an outline of the legislation governing the interception of prisoners' communications, gives details of our prison inspection regime and summarises the key findings from our inspections.

**10.2** Our non-statutory oversight of the interception of communications in prisons in England and Wales commenced in 2002 at the request of the then Home Secretary. In 2008 IOCCO was invited by the then Director General of Northern Ireland prisons to undertake inspections of the Northern Ireland prisons. IOCCO does not currently provide any oversight in respect of Scottish prisons.

## Prison Legislation

**10.3** 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, 43/2014, 10/2015) that impact on this area. In recent years we have pointed out 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. After many years in development we were pleased that in July 2016 the National Offender Management Service (NOMS) issued an interception PSI (04/2016). Regrettably it does not consolidate all other PSIs that relate (in part) to the interception of prisoners' communications. In our view this is a missed opportunity to streamline and provide much needed clarity to the prisons operating the interception policies. It does however represent a welcome step forward in a number of areas, for example, the PSI provides a standardised interception risk assessment template for prisons to use to authorise and review the interception of prisoners' communications. It also requires prisons to maintain electronic logs of any monitoring that is undertaken.

**10.4** 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 will accept our recommendations based on PSIs issued to establishments in England and Wales. For a number of years we have reported that this arrangement is far from ideal and we again recommend that the Northern Ireland Prison Service should issue a comprehensive Instruction to Governors to supplement the Northern Ireland Prison Rules in relation to the interception of prisoners' communications.

**10.5** In our 2015 report the former Commissioner made it clear that it would be preferable if our prison oversight was formalised as a statutory function. Our understanding is that the Government intended to do this under the IP Bill.[65] However, although clause 47 of the IP Bill provides that the interception of communications in a prison is authorised if it is conduct in exercise of any power conferred by or under Prison Rules, there appears to be no provision for this type of interception to be overseen. The IP Bill (clause 205) sets out the main oversight functions of the Investigatory Powers Commissioner and this

65 See version of IP Bill introduced in the House of Lords on 8 June 2016 -http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

includes the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc.) and the exercise of functions by virtue of sections 1 to 4 of the Prisons (Interference with Wireless Telegraphy) Act 2012. Both of these are new areas of oversight which we have not yet started to undertake as we have only so far been informally asked by the Home Office and the Ministry of Justice to oversee their use. We have agreed to, subject to receiving a formal direction from the Prime Minister and some additional resource. It seems odd that these new areas of oversight are provided for in the IP Bill, but that there appears to be no oversight provisions covering our current oversight regime of the interception of prisoners' communications (conduct which will take place under Chapter 2 of Part 2 of the IP Bill). We recommend that this is remedied by an amendment to clause 205 of the IP Bill.

## Authorisations to Intercept Prisoners' Communications

**10.6** **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 Rule 35A(4) (or Northern Ireland Prison Service Prison Rule 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.

**10.7** **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.

**10.8** **Types of monitoring.** Interception is mandatory in some cases, for example, in the case of 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 a 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.

**10.9** Communications which are subject to legal privilege are protected and there are also special arrangements in place for dealing with confidential matters, such as contact with the Samaritans or a prisoner's constituency MP.

**10.10** In November 2014 Her Majesty's Inspectorate of Prisons (HMIP) was asked by the former Minister of Justice to *"investigate the circumstances surrounding the interception of telephone calls from prisoners in England and Wales to the offices of Members of Parliament (MPs), and to make recommendations to ensure that there are sufficient safeguards in place to minimise the risk of such calls being recorded inappropriately in the future"*. HMIP's report[66] was published in July 2015 and they concluded that there was no evidence of a widespread, deliberate attempt to monitor prisoners communications with MPs and that the majority of MPs calls had been listened to in error. We were pleased to note that the report acknowledged the weaknesses that we have identified over a number of years in the systems and processes for protecting confidential calls. In the last 4 years we have made nearly 380 recommendations in this area. HMIP's recommendations also address a number of the concerns and inadequacies that we have identified over a number of years with the policies, training and awareness. We hope that the HMIP inquiry report and recommendations will assist NOMS and the prisons to improve the systems and procedures and to ensure that there are adequate protections in place for communications between prisoners and their MPs and other confidential organisations (e.g. legal calls). We note HMIP's concerns that arrangements put in place to prevent the recording of MPs calls will not be sufficiently well managed to remain effective over time. We will continue to pay close attention during our inspections to the sufficiency of the arrangements in place to protect prisoners communications with MPs and other confidential organisations.

## Inspection Regime

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

**10.12** **Number of inspections.** In 2015 our office conducted 74 inspections at 71 individual prisons. This is just over half of the establishments in England, Wales and Northern Ireland.

**10.13** The length of each inspection depends on the category and capacity of the prison

66 https://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2015/07/prison-communications-report-web-2015.pdf

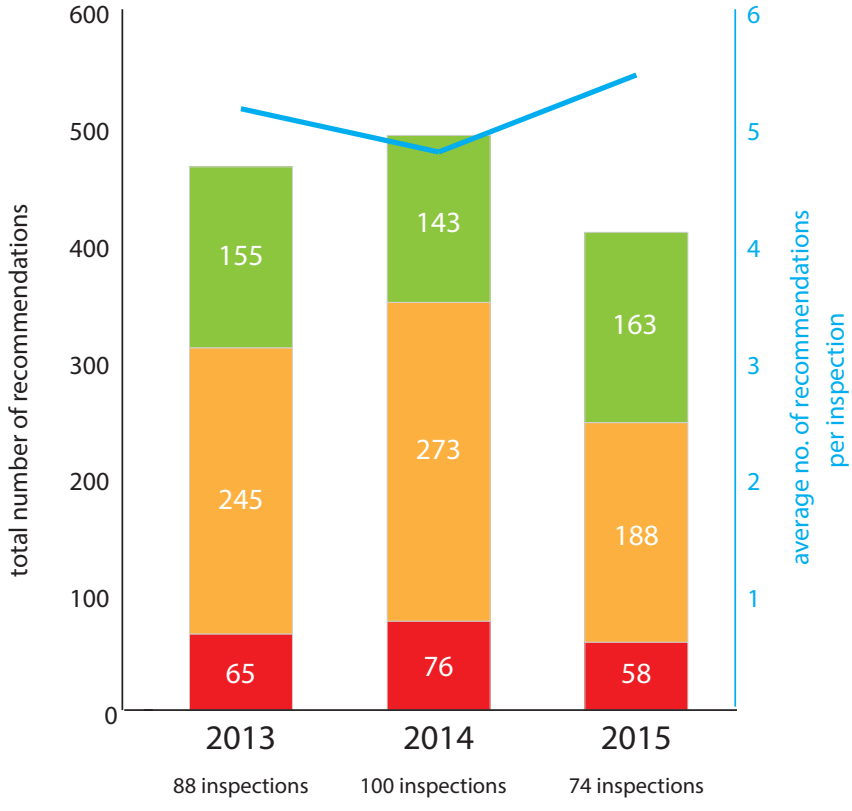
being inspected. The majority of the inspections take place over one day. Inspections of the larger capacity or high security (Category A) prisons may take place over two days.

**10.14 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 and 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.

**10.15 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 state that the recommendations have been implemented, or what progress has been made.

**Figure 17** *Total red, amber & green recommendations from prison inspections 2013-2015*



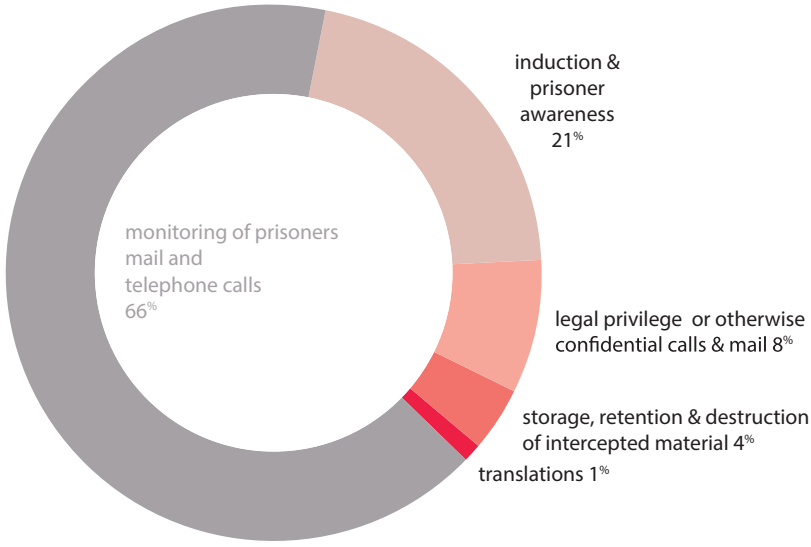
## Inspection Findings & Recommendations

**10.16** The total number of recommendations made during our 74 prison inspections in 2015 was 409, an average of 5.5 recommendations for each prison (**Figure 17**).

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

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

**Figure 18** *2015 prison inspection recommendations by category*




**10.18** In 2015 14% of the recommendations were red, 46% amber and 40% green. **Figure 18** shows the breakdown of the 2015 recommendations by category. As identified in 2014, the majority (66%) of recommendations made during 2015 inspections fell into one key category – the procedures for the monitoring of prisoners' telephone calls and mail. Whilst this category covers a wide range of issues regarding monitoring processes the most significant concerns were around the authorisation and review procedures and

the effectiveness of the monitoring. We again found this year that the necessity and proportionality justifications for invoking or reviewing monitoring in the risk assessments and authorisations had frequently not been made out to a sufficient standard to the extent that it was difficult to see how a Governor had been able to make an informed decision as to whether the monitoring was necessary and proportionate based on the information in the authorisations alone. This concern was particularly prevalent in relation to prisoners who pose a risk to the public e.g. those convicted of harassment offences or those identified as a risk to children.

**10.19** During the inspections we compare the monitoring logs against the call records on the system to check that all of the necessary monitoring had been conducted by monitoring staff. In some cases we identified that not all of the calls made by the prisoners subject to monitoring were being listened to or that the calls were not being listened to in a timely fashion. This is of concern because a significant piece of intelligence could be missed completely or not reacted to promptly, leading to a serious incident occurring which may have otherwise been prevented. Consequently we made a number of recommendations including for the managers to undertake regular audits to check that the necessary monitoring is taking place. The inspectors also made a number of recommendations for prisons to improve the quality of the monitoring logs completed by staff. On this point the new PSI (04/2016) requires logs to be completed electronically rather than by hand. It is important for monitoring staff to complete good quality summaries of a prisoner's communications in the logs as this will help to inform subsequent reviews about whether it is necessary or proportionate to continue monitoring.

**10.20** 21% of recommendations related to prisoner induction and awareness of the monitoring procedures. In particular IOCCO inspectors commonly found in 2015 that prisoner and staff awareness of the full range of confidential access organisations (e.g. MPs, HMIP, Samaritans, Criminal Cases Review Commission) was insufficient. A number of recommendations were made for staff to draw prisoners' attention to the list of confidential organisations when they sign the communications compact and to ensure adequate signage on the pin-phones[67] and mailboxes. A further 8% of recommendations concerned legally privileged or otherwise confidential calls and again the focus was on increasing staff awareness about confidential access organisations among those who administer the pin-phone system to prevent possible occurrences of confidential access telephone numbers being enabled on the "open" side of the system, which would result in the calls being recorded and potentially listened to.

**10.21** Under Prison Rules the intercept product (i.e. copies of calls and mail) can only be retained for three months unless its ongoing retention is authorised by a Governor. 4% of the recommendations concerned the storage, retention and destruction of intercepted material. In the main these related to those prisons who were still utilising DVDs to backup the recorded calls and had failed to overwrite DVDs containing content older than three

67 The pin-phone system is the telephone system which prisoners use to make telephone calls. Each prisoner has his or her own account on the system which is accessed by a pin number. Prisoners are only able to call those numbers enabled on their account by staff. If the number relates to a confidential access organisation it is placed on the "barred" side of the system which means the call is not recorded and cannot be listened to by staff.

months. Most prisons have now migrated to a hard drive system which automatically deletes the calls at the three month point. The inspectors also found by checking the prison's email inboxes and sent items folder that in a number of cases records relating to the '*emailaprisoner*' service had also been retained in excess of the three month period.

**10.22** The final 1% of recommendations (4 recommendations) concerned prisons not having an adequate translation strategy in place to deal with calls or correspondence in a foreign language. This was particularly relevant to those prisons with a high proportion of foreign national prisoners where a small number of inspections revealed that staff were being directed to listen to a large number of calls made in foreign languages but were not being provided with any guidance as to whether the calls should be translated. Consequently no benefit was being derived from the monitoring which undermines the necessity and proportionality for it as the exercise cannot meet the objective for which monitoring was authorised.

**10.23** At the end of each inspection, each prison is given an overall rating (good, satisfactory, poor). This rating is determined by considering the total number of recommendations made, the severity of those recommendations, and whether recommendations made following a previous inspection had to be carried forward because they were not achieved. In 2015 54 (73%) of prisons achieved a good rating, 8 (11%) were satisfactory, and 12 (16%) were poor. Whilst this is broadly similar with previous years, comparisons are difficult because the prisons being inspected are not the same. With regard to whether recommendations made following a previous inspection had to be carried forward, 87% of prisons inspected in 2015 that received recommendations in their previous inspection had fully achieved all or the majority of those recommendations.

**10.24** A more reliable way to gauge whether compliance is improving is to compare each prison's level of compliance from its 2015 inspection to its previous inspection rating:

- 45 inspections resulted in the level of compliance remaining the same, with 39 prisons continuing to achieve a good level of compliance, 4 satisfactory and 2 poor.
- 16 inspections resulted in the prisons improving their rating, with 6 prisons moving from satisfactory to good, 9 from poor to good, and 1 from poor to satisfactory.
- 13 inspections resulted in the compliance rating worsening, with 3 prisons moving from good to satisfactory, 7 from good to poor, and 3 from satisfactory to poor.

**10.25** The inspectors found that changes in compliance often reflect changes to the resourcing and management of this function within the prisons (e.g. moving from a dedicated experienced team undertaking monitoring to a duty shared amongst a greater number of staff). Such changes can have a considerable impact in a short space of time and reinforces the need for prison Governors to assess periodically between inspections that the interception of prisoners' communications is being carried out effectively.

# Points of Note

### Prisons

We continue to provide non-statutory oversight of the interception of communications in prisons in England, Wales and Northern Ireland.

Our understanding is that the Government intends to place our oversight on a statutory footing under the Investigatory Powers Bill (IP Bill). However this function appears at present to be omitted from the oversight clauses in the IP Bill. Curiously the IP Bill clauses do however include two new areas of oversight in prisons which we have not yet started to undertake (relating to the Prisons (Interference with Wireless Telegraphy) Act 2012 and section 80 of the Serious Crime Act 2015). We recommend this is remedied by an amendment to clause 205 of the IP Bill.

In 2014 we conducted 74 prison inspections. 409 recommendations emanated from those inspections, an average of 5.5 recommendations for each prison.

87% of the recommendations fell into two key categories: the procedures for the monitoring of prisoners telephone calls and mail, and prisoner induction and awareness of the monitoring procedures.

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. A more reliable way is to compare each prison's level of compliance to their previous inspection. In 2015 45 prisons maintained the same level of compliance (of which 39 were 'good'), 16 improved and 13 worsened. 87% of prisons inspected that received recommendations in their previous inspection had fully achieved all or the majority of those recommendations.

After many years in development we were pleased that recently (in July 2016) the National Offender Management Service (NOMS) issued an interception Prison Service Instruction (PSI) (04/2016). Regrettably the PSI does not consolidate all other PSIs that relate (in part) to the interception of prisoners communications. This in our view is a missed opportunity to streamline the policy in this area and provide much needed clarity. It does however represent a welcome step forward in a number of areas.

# Annex A: Public Authorities with Powers to Acquire Communications Data under Chapter 2 of Part 1 of RIPA

| 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<br>- 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<br>- Royal Air Force Police<br>- Royal Military Police<br>- Royal Naval Police | • | • | • | • | • | • | | | | • | | | | |
| - Civil Nuclear Constabulary | • | • | • | • | • | | | | | | | | | |
| - Port of Dover Police<br>- Port of Liverpool Police | • | • | • | | • | | • | • | | | | • | | (d) & (e) subscriber only |
| - Gambling Commission<br>- Gangmasters Licensing Authority<br>- The Information Commissioner<br>- Office of Communications<br>- Police Ombudsman for Northern Ireland<br>- Royal Mail Group<br>- Serious Fraud Office | • | • | • | | • | | | | | | | | | |
| - Financial Conduct Authority<br>- Prudential Regulation Authority | • | • | • | | • | | | | | | | | • | Statutory purpose Art.2(c) was made available from 12/02/15 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - Independent Police Complaints Commission<br>- Police Investigations and Review Commissioner | • | • | • | | • | | | | | | | • | | |
| - The Ministry of Justice - National Offender Management Service<br>- Northern Ireland Office - Northern Ireland Prison Service | • | • | • | | • | | • | | | | | • | | (d) subscriber only |
| - Criminal Cases Review Commission<br>- Scottish Criminal Cases Review Commission | • | • | • | | | | | | | | • | | | |
| Department of Transport:<br>- Air Accident Investigation Branch<br>- Marine Accident Investigation Branch<br>- Rail Accident Investigation Branch | • | • | • | | | | • | | | | | | | |
| - Department for Transport Maritime Coastguard Agency<br>- Fire & Rescue Authorities<br>- Ambulance Services / Trusts | • | • | • | | • | | • | | | • | | | | (b) service use & subscriber only<br>(d) subscriber only.<br>(g) traffic, service use & subscriber |
| - Environment Agency<br>- Health & Safety Executive<br>- Department for Health - Medicines & Healthcare Products Regulatory Agency<br>- Scottish Environment Protection Agency | | • | • | | • | | • | • | | | | | | (d) & (e) subscriber only |
| - Food Standards Agency | | • | • | | • | | | • | | | | | | (e) subscriber only |
| - Charity Commission<br>- DWP – Child Maintenance Group<br>- Department of Agriculture & Rural Development (Northern Ireland)<br>- Department for Business Innovation & Skills<br>- Department for Environment Food & Rural Affairs<br>- Department of the Environment Northern Ireland<br>- Health & Social Care Business Services Organisation - Central Services Agency (Northern Ireland)<br>- Competition and Markets Authority<br>- Pensions Regulator<br>- NHS Protect<br>- NHS Scotland Counter Fraud Services<br>- 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 Items of Communications Data under Chapter 2 of Part 1 of RIPA by Public Authority

This Annex details the total items of data approved by each public authority in 2015.

Public authorities have only been required to provide statistical details about the number of items of data since 25 March 2015 when the revised Code of Practice came into force. Consequently, some public authorities have only been able to give the total items of data approved from the 1 April 2015 (three quarters of the year), rather than from the 1 January (the full four quarters of the year). Where this is the case, and in order to provide comparable figures the three quarter totals have been 'projected' to make up the difference simply by multiplying it by 1.333r. Our analysis shows that the use of these powers remains constant throughout the year and so we are confident that the projections provide a more accurate picture of use than the limited statistics of previous years. Any statistics that have been projected are shown in red and the three quarter figure reported by the public authority is displayed in the adjacent column.

## The Intelligence Services

| | Total items of data (projected) | Partial figure reported 01/04/15-31/12/15 |
|---|---|---|
| Government Communications Headquarters (GCHQ) | 4,268 | 3201 |
| Secret Intelligence Service (SIS) | 531 | - |
| Security Service | 38,317 | - |
| Grand Total | **43,116** | |

## Police Forces & Law Enforcement Agencies

| | Total items of data (projected) | Partial figure reported 01/04/15-31/12/15 |
|---|---|---|
| Avon & Somerset Constabulary | 15,277 | 11,458 |
| Bedfordshire Police | 3,791 | 2,843 |
| British Transport Police | 2,900 | 2,175 |
| Cambridgeshire Constabulary | 4,109 | 3,082 |
| Cheshire Constabulary* | 10,604 | 7,953 |
| City of London Police | 4,065 | 3,049 |
| Cleveland Police | 10,852 | 8,139 |
| Cumbria Constabulary | 3,876 | - |
| Derbyshire Constabulary | 6,459 | - |
| Devon & Cornwall Police | 20,895 | 15,671 |
| Dorset Police | 3,739 | 2,804 |
| Durham Constabulary | 7,676 | - |
| Dyfed Powys Police | 3,104 | 2,328 |
| Gloucestershire Constabulary | 2,756 | 2,067 |
| Greater Manchester Police | 33,143 | 24,857 |
| Gwent Police | 5,315 | 3,986 |
| Hampshire Constabulary | 12,813 | - |
| Hertfordshire Constabulary | 14,581 | - |
| Her Majesty's Revenue & Customs (HMRC) | 12,191 | - |
| Humberside Police | 5,436 | 4,077 |
| Kent Police & Essex Police** | 20,067 | - |
| Lancashire Constabulary | 19,672 | 14,754 |
| Leicestershire Police | 8,637 | 6,478 |
| Lincolnshire Police | 4,444 | 3,333 |
| Merseyside Police | 24,780 | 18,585 |

| | Total items of data (projected) | Partial figure reported 01/04/15-31/12/15 |
|---|---|---|
| Metropolitan Police Service | 107,362 | |
| Ministry of Defence Police | 136 | - |
| National Crime Agency (NCA) | 64,116 | 48,087 |
| Norfolk Constabulary & Suffolk Police** | 6,499 | 4,874 |
| North Wales Police | 6,928 | |
| North Yorkshire Police | 5,269 | 3,952 |
| Northamptonshire Police | 7,063 | - |
| Northumbria Police | 9,853 | - |
| Nottinghamshire Police | 16,762 | - |
| Police Service of Scotland | 51,719 | - |
| Police Service of Northern Ireland (PSNI) | 8,813 | 6,610 |
| Royal Air Force Police | 9 | 7 |
| Royal Military Police | 356 | - |
| Royal Navy Police | 45 | 34 |
| South Wales Police | 17,368 | 13,026 |
| South Yorkshire Police | 8,225 | 6,169 |
| Staffordshire Police | 9,350 | - |
| Surrey Police | 8,896 | 6,672 |
| Sussex Police | 5,305 | 3,979 |
| Thames Valley Police | 11,983 | 8,987 |
| Home Office (Immigration Enforcement) | 6,113 | 4,585 |
| Warwickshire Police & West Mercia Police** | 18,996 | - |
| West Midlands Police | 45,238 | - |
| West Yorkshire Police | 31,673 | 23,755 |
| Wiltshire Police | 4,472 | 3,354 |

| Grand Total | **713,731** |
|---|---|

*Cheshire Constabulary's total items do not include items approved orally, so will be higher than the figures presented.

**Some police forces share the services of a SPoC, and where this is so combined figures are reported.

Having lost their powers on 12 February 2015, the Civil Nuclear Constabulary, the Port of Dover Police and the Port of Liverpool Police all reported that they did not approve any items of data between 1 January and 12 February 2015.

## Other Public Authorities

| | Total items of data (projected) | Partial figure reported 01/04/15-31/12/15 |
|---|---|---|
| Air Accident Investigation Branch | 21 | - |
| Competition and Markets Authority | 87 | - |
| Criminal Cases Review Commission | 11 | - |
| Department of Enterprise, Trade & Investment (Northern Ireland) | 101 | 76 |
| Department of Work & Pensions - Child Maintenance Group | 14 | - |
| Financial Conduct Authority | 2,808 | - |
| Gambling Commission | 36 | - |
| Gangmasters Licensing Authority | 82 | - |
| Health & Safety Executive | 7 | - |
| Independent Police Complaints Commission | 30 | - |

| | Total items of data (projected) | Partial figure reported 01/04/15-31/12/15 |
|---|---|---|
| Information Commissioner's Office | 24 | - |
| Maritime and Coastguard Agency | 6 | - |
| Medicines and Healthcare Products Regulatory Agency | 228 | 171 |
| Ministry of Justice - National Offender Management Service | 75 | - |
| NHS Protect | 16 | - |
| Office of Communications | 27 | - |
| Office of the Police Ombudsman for Northern Ireland | 18 | - |
| Rail Accident Investigation Branch | 11 | - |
| Royal Mail* | 28 | |
| Serious Fraud Office | 250 | - |

| Grand Total | **3,880** |
|---|---|

*Royal Mail lost its powers to acquire communications data on 12/02/2015 and the figure reported here represents items acquired between 01 January and 12 February 2015.

The following "other" public authorities reported that they did not acquire any communications data during 2015 (those in orange also lost their powers on 12/02/2015):

- Charity Commission
- Department for the Environment, Food & Rural Affairs
- Department for Business, Innovation & Skills
- Department of the Environment (Northern Ireland)
- Department of Agriculture & Rural Development (Northern Ireland)
- Environment Agency
- Food Standards Agency
- Marine Accident Investigation Branch
- NHS Scotland
- Northern Ireland Health & Social Services Central Services Agency
- Northern Ireland Office - Northern Ireland Prison Service
- Police Investigations Review Commissioner
- Prudential Regulation Authority
- Scottish Criminal Cases Review Commissioner
- Scottish Environmental Protection Agency
- The Pensions Regulator
- No Fire Authority
- No Ambulance Service or Trust

## Local Authorities

| | Total items of data |
|---|---|
| Aberdeenshire Council | 2 |
| Barnsley Metropolitan Council | 9 |
| Bedford Borough Council | 4 |
| Birmingham City Council | 52 |
| Bracknell Forest Borough Council | 1 |
| Bristol City Council | 2 |
| Bromsgrove District Council | 30 |
| Buckinghamshire County Council | 7 |
| Bury Metropolitan Borough Council | 2 |
| Caerphilly County Borough Council | 3 |
| Cambridgeshire County Council | 4 |
| Cardiff City and County Council | 15 |
| Ceredigion County Council | 2 |
| Cheshire East Council | 4 |
| Cheshire West & Chester Council | 9 |
| City of London Corporation | 13 |
| Cornwall County Council | 15 |
| Darlington Borough Council | 6 |
| Devon County Council | 19 |
| Dudley Metropolitan Council | 10 |
| Durham County Council | 37 |
| East Riding of Yorkshire Council | 9 |
| Flintshire County Council | 1 |
| Gateshead Metropolitan Borough Council | 15 |
| Glasgow City Council | 2 |
| Gloucestershire County Council | 12 |
| Hampshire County Council | 3 |
| Hertfordshire County Council | 5 |
| Hertsmere Borough Council | 2 |
| Huntingdonshire District Council | 5 |
| Kent County Council | 107 |
| Lancashire County Council | 15 |
| Leicestershire County Council | 71 |
| Lincolnshire County Council | 6 |
| London Borough of Brent | 2 |
| London Borough of Bromley | 55 |

| | Total items of data |
|---|---|
| London Borough of Camden Council | 1 |
| London Borough of Croydon Council | 31 |
| London Borough of Enfield Council | 3 |
| London Borough of Harrow Council | 3 |
| London Borough of Redbridge Council | 8 |
| Merthyr Tydfil County Borough Council | 3 |
| Milton Keynes Borough Council | 3 |
| North Kesteven District Council | 8 |
| North Lincolnshire Council | 6 |
| North Yorkshire County Council | 4 |
| Northamptonshire County Council | 6 |
| Northumberland County Council | 14 |
| Nottinghamshire County Council | 15 |
| Oldham Metropolitan Borough Council | 4 |
| Oxfordshire County Council | 31 |
| Poole Borough Council | 7 |
| Portsmouth City Council | 8 |
| Redcar & Cleveland BC | 30 |
| Rhondda Cynon Taff County BC | 41 |
| Rotherham Borough Council | 1 |
| Shropshire Council | 6 |
| South Gloucestershire Council | 1 |
| Staffordshire County Council | 61 |
| Stockport Metropolitan Borough Council | 2 |
| Stockton-on-Tees Borough Council | 5 |
| Stoke-on-Trent City Council | 13 |
| Suffolk County Council | 21 |
| Swindon Borough Council | 5 |
| Thurrock Borough Council | 18 |
| Torfaen County Borough Council | 3 |
| Warrington Borough Council | 16 |
| Warwickshire County Council | 3 |
| Wealden District Council | 4 |
| West Berkshire Council | 14 |
| Wrexham County Borough Council | 6 |
| York City Council | 14 |

| Grand Total | **975** |
|---|---|

## Statistical limitations in main report

**Items of data (Paragraph 7.22).** Where a public authority has only been able to provide figures (such as the total number of items of data acquired) for 3 quarters of 2015 (due to the fact that the new statistical requirements did not come into effect until the end of the first quarter), this figure has been projected by simply multiplying it by 1.333 recurring.

**By type of data under section 21(4) of RIPA (Paragraph 7.23).** This breakdown excludes 3 public authorities who were unable to accurately breakdown items of data acquired under the urgent oral procedures.

**By data description (identifier) (Paragraph 7.24).** This breakdown excludes 8 public authorities who were unable to provide this breakdown down either at all, or for items relating to the urgent oral procedures.

**Person type (Paragraph 7.29).** These figures are based on a partial sample of 664,848 items of data. The remaining items (c.100,000 items) were not categorised by public authorities. This was due either to staff omitting to categorise or the system not being configured to capture this information. In many instances (c.30,000 items) the omission is confined to the items of data acquired during the urgent oral process. Given the fact that the majority of urgent oral requests related to tracing vulnerable missing persons, it is likely that the vulnerable person category would be of parity with the victim and associate categories.

**Age of items of data requested (Paragraph 7.30).** The analysis provided in the main report is based on a partial sample of 96,292 items of data submitted by 40 public authorities where the figures equalled the total items of data acquired and therefore are considered to be reliable. The remaining public authorities were unable to provide reliable figures for a number of reasons, for example:

- those utilising one of the major application workflow systems could only produce an average figure per application rather than a value for each individual item;
- a large number of items did not have a date recorded against them and so it was not possible for an age to be calculated (e.g. the request was simply for 'current subscriber information');
- some public authorities had not captured this statistical information in acquisitions undertaken outside the main workflow system (e.g. under the urgent oral process)
- 5 public authorities were utilising a workflow system during the reporting period which was not configured to capture this information at all.

**Periods of data acquired (Paragraph 7.31).** For similar reasons to those given in the preceding category, the analysis in the report is based on a partial sample of 104,182 items acquired by 39 public authorities.

# Annex C: Budget

The 2015/16 budget of £1,101,000 was allocated as below:

### 2015/16 Expenditure

| Description | Total (£) | Actual Expenditure (£) |
|---|---|---|
| Staff Costs | 978,000 | 828,961 |
| Travel & Subsistence | 93,000 | 86,307 |
| IT and Telecoms | 2,000 | 1,839 |
| Training & Recruitment | 10,000 | 9,023 |
| Office supplies, stationery, printing | 15,000 | 20,034 |
| Conferences & Meetings | 500 | 190 |
| Other | 2,500 | 1,272 |
| Total | 1,101,000 | 947,626 |

### 2014/15 Expenditure

| Description | Budget (£) | Actual Expenditure (£) |
|---|---|---|
| Staff Costs | 919,900 | 917,798 |
| Travel & Subsistence | 117,000 | 81,917 |
| IT and Telecoms | 5,600 | 2,989 |
| Training & Recruitment | 15,800 | 11,800 |
| Office supplies, stationery, printing | 6,000 | 10,187 |
| Conferences & Meetings | 7,300 | 318 |
| Other | 2,500 | 3,577 |
| Total | 1,074,100 | 1,028,586 |

# Annex D: Glossary of Terms & Abbreviations

| Term | Explanation |
|---|---|
| CPIA | Criminal Procedure and Investigations Act 1996 |
| CSP | Communication Service Provider |
| CTIVD | Dutch Review Committee on the Intelligence and Security Services |
| DCG | Data Communications Group |
| DP | Designated Person |
| DRIPA | Data Retention and Investigatory Powers Act 2014 |
| ECHR | European Convention on Human Rights |
| ECJ | European Court of Justice |
| FCO | Foreign and Commonwealth Office |
| GCHQ | Government Communications Headquarters |
| HMIP | Her Majesty's Inspectorate of Prisons |
| HMRC | Her Majesty's Revenue & Customs |
| HRA | Human Rights Act |
| ICDDF | International Communications Data and Digital Forensics Conference |
| IOCCO | Interception of Communications Commissioner's Office |
| IP Bill | Investigatory Powers Bill |
| IPT | Investigatory Powers Tribunal |
| ISC | Intelligence and Security Committee of Parliament |
| MOD | Ministry of Defence |
| MPS | Metropolitan Police Service |
| NAFN | National Anti-Fraud Network |
| NCA | National Crime Agency |
| NOMS | National Offender Management Service |
| NPCC | National Police Chiefs' Council |
| NSF | National Security Framework |
| NTAC | National Technical Assistance Centre |
| PSD | Professional Standards Department |
| PSI | Prison Service Instruction |
| PSNI | Police Service Northern Ireland |
| RIPA | Regulation of Investigatory Powers Act 2000 |
| RUSI | Royal United Services Institute |
| SIO | Senior Investigating Officer |
| SIS | Secret Intelligence Service |
| SPoC | Single Point of Contact |
| SRO | Senior Responsible Officer |

ISBN 978-1-4741-3639-6