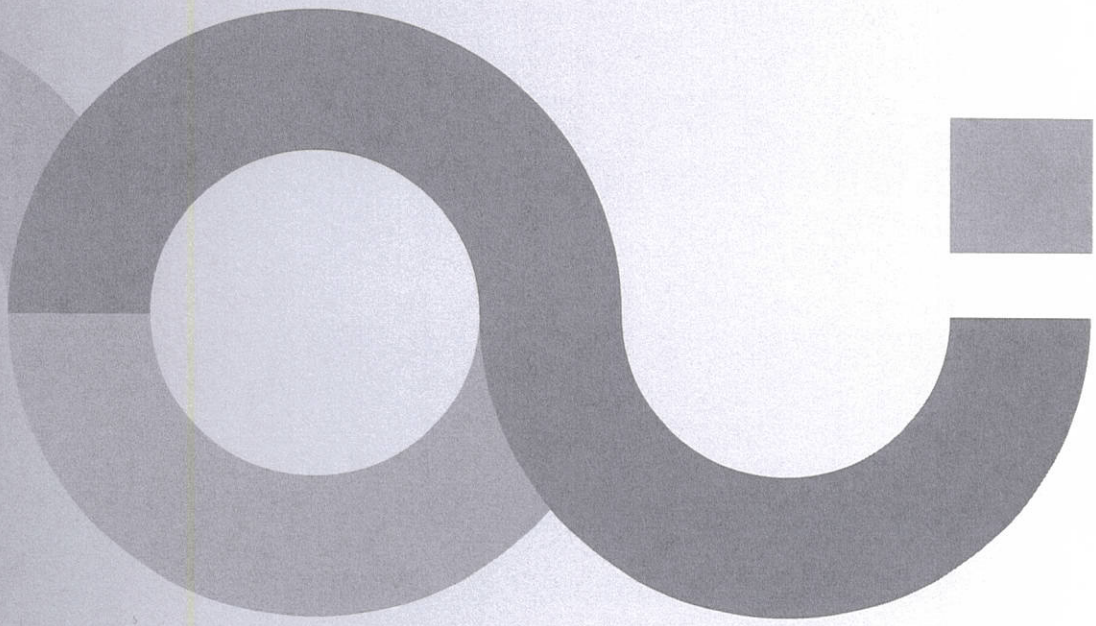
Report of the Interception of Communications Commissioner

Annual Report for 2016

(covering the period January to December 2016)

The Rt Hon.
Sir Stanley Burnton



Report of the Interception of Communications Commissioner

Annual Report for 2016
(covering the period January to December 2016)

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 20 December 2017

Laid before the Scottish Parliament by the Scottish Ministers on 20 December 2017

HC 297
SG/2017/77

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated.
To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

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

Any enquiries regarding this publication should be sent to: info@ipco.gsi.gov.uk

ISBN 978-1-5286-0174-0

CCS1217634744 12/17

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

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

31 July 2017

Dear Prime Minister,

I am required by section 58(4) of the Regulation of Investigatory Powers Act (RIPA) 2000 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. In 2016, my inspectors and I carried out 166 inspections of 134 public authorities. We were notified of 1,200 errors, and conducted investigations into 29 serious errors.

This represents a huge amount of work by my office (IOCCO). I would like formally to thank my team for their efforts. I would also like to express my appreciation for the work of the hundreds of people we have inspected at Public Authorities across the UK. As well as their important work on compliance, our colleagues in Government are also responsible for keeping the public safe: finding vulnerable missing people, uncovering terrorist plots, and catching criminals.

In general, the standard of compliance is high. Errors and more general problems form a very small percentage of the total activity I inspect. However, 2016's inspections have raised one area of significant concern. This report includes a specific chapter on errors occurring during IP Address Resolutions. These are far more common than is acceptable, especially in cases relating to Child Sexual Exploitation. The impact on some victims of these errors has been appalling.

The key event impacting my work in 2016 was the passage of the Investigatory Powers Act. I have given some detailed thoughts on the IPA in this report. The judicial 'double-lock', which applies to many of the powers I oversee, is a significant change in the nature of oversight.

Under previous legislation, any concerns that Commissioners have had about conduct or legal interpretation might have been reflected in recommendations to the authority in question and then in public in the annual report. Apart from in the case of some communications data errors, commissioners have had minimal powers of sanction. In the future, unless a judicial commissioner is convinced of the lawfulness of a course of action, it will not happen.

This increased oversight brings with it a number of challenges. The Investigatory Powers Commissioner will be more closely involved in ongoing operations than I and my predecessors have been. I welcome the Government's commitment to enabling

'world-leading oversight' by properly resourcing and supporting the Commissioner. This is important for the quality of oversight, but also to prevent the Commissioner's office becoming a bottleneck for important investigative activity.

This will be the last annual report produced by an Interception of Communications Commissioner. My functions will move under the Investigatory Powers Commissioner later this year. I would like to reiterate my thanks to you for appointing me to this fascinating role, and to wish Lord Justice Adrian Fulford every success as the Investigatory Powers Commissioner.

Yours sincerely,

The Rt Hon. Sir Stanley Burnton
Interception of Communications Commissioner

Contents

IOCCO's Role **1**

Communications Data **3**

Communications Data legislation 3

National Anti-Fraud Network 5

Statistics 6

Inspection Regime 13

Inspection Findings and Recommendations 14

Principal Recommendations and Key Issues 15

Communications Data Errors **17**

Error Statistics 17

Serious Error Investigations 18

Summary of Serious Investigations 20

Errors 21

IP Address Resolution Errors **21**

Bulk Communications Data **25**

Bulk Communications Data 26

Update to my review report 26

Applications for section 94 directions 27

Access to the bulk communications data retained by the agency 28

Errors 30

Interception of Communications **32**

Applications for Interception Warrants 32

Interception Warrants 34

Statistics for Interception Warrants 38

Inspection Regime 40

Inspection Recommendations and Observations 44

Application Process 44

Changes to the GCHQ interception inspection regime 45

Interception Errors **47**

Prisons **50**

The Investigatory Powers Act **54**

Annex A: Number of Communications **56**

Annex B: Public Authorities' **62**

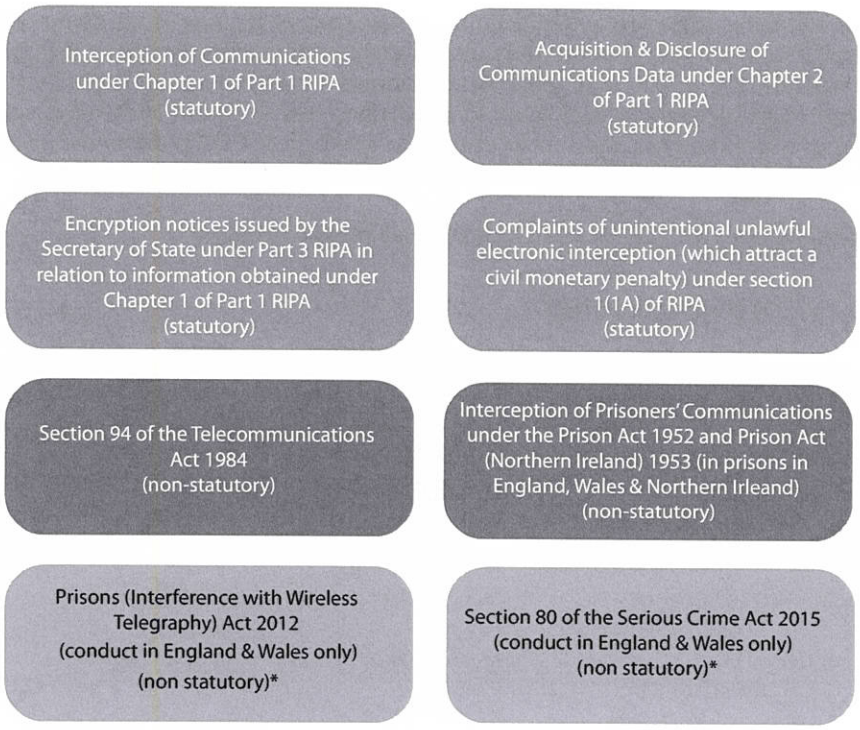
Annex C: Prisons Inspection Scores **65**

Annex D: Serious Errors **66**

IOCCO's Role

The Interception of Communications Commissioner's principal duty is to review 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). I also undertake a number of other oversight functions, some of which are carried out on a non-statutory basis. I report on my activities, on a yearly basis, to the Prime Minister. Since 2013, these reports have been published in full with no confidential annex. My role is not to be a champion of the Government or the law but to provide independent oversight of how the law is applied.

Figure 1 *Describes the Powers that the Commissioner oversees.*



*We have 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.

I oversee an extensive inspection regime that enables me to carry out effective oversight. Section 58(1) of RIPA imposes a statutory obligation on every public official in an organisation which has the powers I oversee to disclose or to provide to the Commissioner all such documents or information as may be required for the purpose of enabling the Commissioner to carry out their functions.

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 or she is properly able to carry out their functions. These staff make up the Interception of Communications Commissioner's Office (IOCCO) – a team of around ten inspectors and two secretarial staff. IOCCO's staff are independent, highly skilled, and experienced in the principles and detail of RIPA. The inspectors have been recruited from a variety of backgrounds and bring with them a broad range of experience. Their expertise covers the fields of legal, policy, analytics 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.

IOCCO is an outward-facing organisation. A key part of its role is to communicate outside of Government: to increase the public understanding of investigative techniques, and to reassure the public that there is appropriate independent oversight of public authorities' investigative activities. During 2016, I and members of IOCCO have spoken at a number of conferences and similar events. In addition, IOCCO published a paper on the Investigatory Powers Bill in advance of its consideration by the House of Lords.

My office's budget for 2016/17 was £1,140,093, allocated as below.

Table A *IOCCO's budget for 2016/17.*

2016/17	Budget	Actual
Staff Costs	£ 1,013,285.00	£ 957,073.02
Travel and Subsistence	£ 98,950.00	£ 116,459.09
IT and Telecomms	£ 4,000.00	£ 837.53
Training and Recruitment	£ 13,500.00	£ 1,172.00
Office Supplies, Stationery, Printing	£ 9,358.00	£ 7,795.66
Conferences and Meetings	£ 1,000.00	£ 5,298.62
Other	-	£ 6,396.00
Total	£ 1,140,093.00	£ 1,095,031.92

Communications Data

This section provides an outline of communications data legislation, gives details of the communications data inspection regime, provides statistical information about the use of communications data by public authorities and identifies key findings from IOCCO's inspections.

Communications Data legislation

Chapter 2 of Part 1 of RIPA (sections 21 to 25) and the Acquisition and Disclosure of Communications Data Code of Practice set out the procedures for the acquisition and disclosure of communications data. Unless otherwise specified, references in this section to 'the Code of Practice' are to that Code.

Communications data embraces the 'who', 'when' and 'where' of a communication, but not the content of what was said or written. In essence, communications data comprises 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 it was sent; the time at which it was sent; and other related material *(see sections 21(4)(a) and 21(6) and (7) RIPA and paragraphs 2.24 to 2.27 of the Code of Practice).* Examples of this would be email headers and data relating to the location of a mobile phone (cell-site data).
- 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 appears on Communications Service Provider's (CSP's) itemised billing documents *(see Section 21(4)(b) RIPA and paragraphs 2.23 and 2.28 to 2.29 of the Code of Practice).* Examples of this would include the 'to', 'from' and 'duration' of a phone call or text message.
- 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 provides when they sign up to use a service. *(See Section 21(4)(c) RIPA and paragraphs 2.30 and 2.31 of the Code of Practice).* Examples of this would include the name and address of the subscriber of a telephone number or the account holder of an email address.

A number of public authorities have statutory powers to apply for communications data under Chapter 2 of Part 1 of RIPA. These include:

- Police forces;
- The National Crime Agency (NCA);
- Her Majesty's Revenue and Customs (HMRC);
- Intelligence agencies;
- The Gambling Commission;
- The Department for Transport;
- The Home Office (Immigration Enforcement);
- Local Authorities, through the National Anti-Fraud Network (NAFN); and
- The Criminal Case Review Commission.

For a designated person to give lawful authority to acquire communications data within the public authority, there has to be:

- An applicant – who requests the data for the purpose of an investigation *(see paragraph 3.5 of the Code of Practice)*. This would usually be a relatively junior member of an investigative team.
- A designated person (DP) – the holder of a more senior office in the relevant public authority. The DP's function is to decide whether to give authority to acquire the data. Their function and duties are described in paragraphs 3.7 to 3.18 of the Code of Practice. With few exceptions, the DP must be independent of the investigation and is responsible for deciding whether the acquisition is lawful, necessary and proportionate *(see paragraphs 3.7-3.18 of the Code of Practice)*.
- A single point of contact (SPoC) – an accredited person who is trained to facilitate the lawful acquisition of communications data *(see paragraphs 3.19-3.30 of the Code of Practice)*. This person would usually have specific technical expertise. They would usually manage the relationships with Communications Service Providers (CSPs) and with IOCCO.
- A senior responsible officer (SRO) – who is responsible for the integrity of the process and for compliance with Chapter 2 of Part 1 RIPA and the code of practice *(see paragraphs 3.31 of the Code of Practice)*. This would usually be a senior manager of a public authority.

The DP may only give authority to obtain communications data if they believe that it is necessary for one or more of the statutory purposes set out in Section 22(2) of RIPA or subsequent statutory instruments. These require the conduct authorised to be:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic wellbeing of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- 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 themselves 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 themselves, 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; or
- for the purpose of exercising functions relating to the regulation of the financial services and markets or to financial stability.

The statutory purposes for which certain public authorities may acquire communications data and the type of data that they may acquire are restricted. For example, local authorities may only acquire service use and subscriber information for the purpose of preventing or detecting crime or preventing disorder.

In order to justify that an application is necessary, the applicant must address three main points (see paragraphs 2.37-2.38 of the Code of Practice) and establish a link between them:

- the event under investigation, such as a crime or search for a vulnerable missing person;
- the person, such as a suspect, witness or missing person, and how they are linked to the event; and
- the communications data, such as a telephone number or Internet Protocol (IP) address and how the data is related to the person and the event.

DPs may only approve an application if they believe that obtaining the data is proportionate to what the public authority is trying to achieve. Applications must explicitly address the question of proportionality.

A judgment on the question of proportionality requires balancing the necessity of the request for communications data against the likely intrusion into privacy. Considerations should include whether the information which is sought could reasonably be obtained by other less intrusive means. Applications for communications data should not be authorised where it is adjudged that the necessity does not outweigh the intrusion.

National Anti-Fraud Network

The National Anti-Fraud Network (NAFN) is the single point of contact for all local authority acquisition of communications data. 90% of local authorities (LAs)are members of the network, which has over 10,000 users.

NAFN's role is to ensure that members' enquiries are legally compliant and processed in accordance with the most up-to-date information and guidance. The team also provides support and training to its members, and promotes the use of communications data to support their investigations.

All local authorities must make applications for communications data through a SPoC at the National Anti-Fraud Network. The Investigatory Powers Act also provides an opportunity for NAFN to offer its SPoC service to other public bodies through collaboration agreements.

NAFN requested 724 items of data on behalf of local authorities in 2016 and scored a 'good' level of compliance in its inspection.

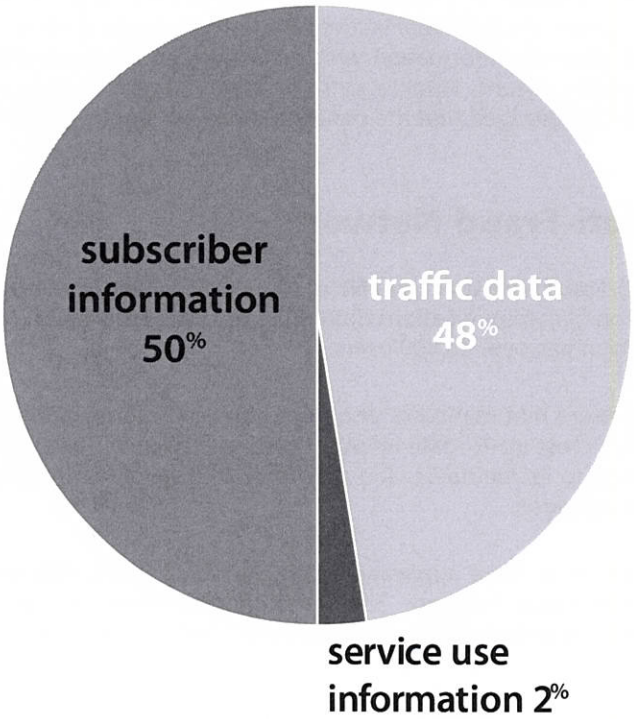
Statistics

The revised March 2015 Code of Practice requires public authorities to interpret and collate statistical requirements in a consistent way. This year's statistical returns represent the first complete reporting period since the introduction of those revised requirements.

Items of Communications Data. 754,559 items of communications data were acquired by public authorities during 2016. An item of data is a request for data on a single communications address 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. Equally, a request for the details of a subscriber to a communications service would be counted as one item of data. The number of items of data acquired by each public authority is detailed in Annex A.

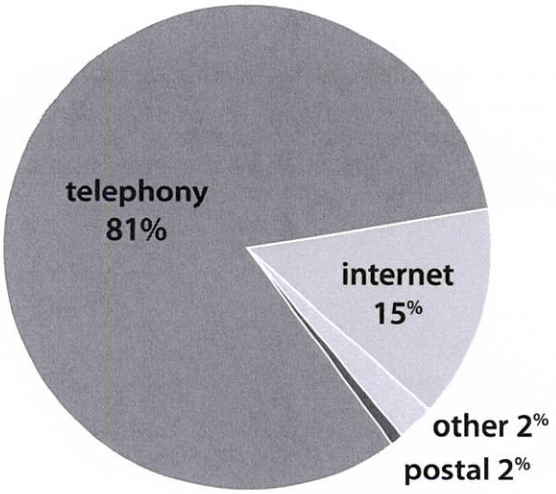
Types of data. 50% of the data acquired was subscriber information, 48% was traffic data and 2% service use information.

Figure 2 *Type of Data.*



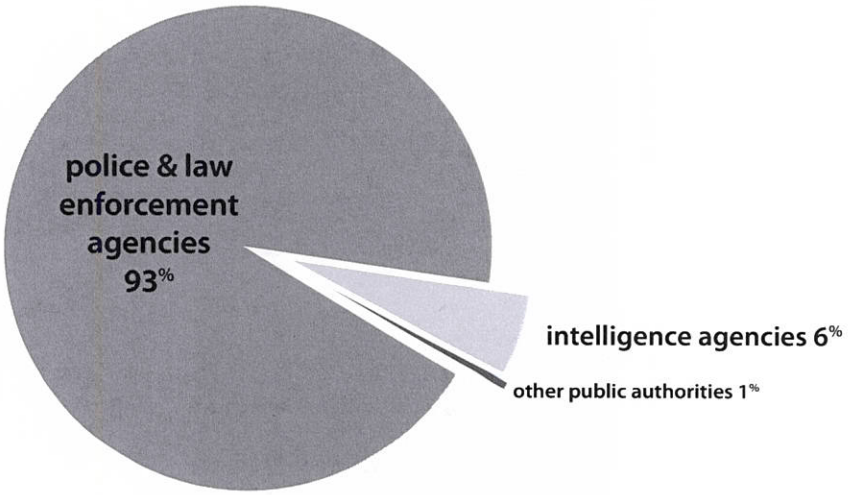
Most of the acquired items of data (81%) related to telephony, such as landlines or mobile phones. Internet identifiers, for example email or IP addresses, accounted for 15% of the acquired data. 2% of requests were related to postal identifiers.

Figure 3 *Type of Data.*



Public Authority Use. Police forces and law enforcement agencies were responsible for acquiring 93% of the total number of items of data in 2016. 6% was acquired by intelligence agencies. The remaining 1% was acquired by other public authorities, including local authorities.

Figure 4 *Items by Public Authority Type.*

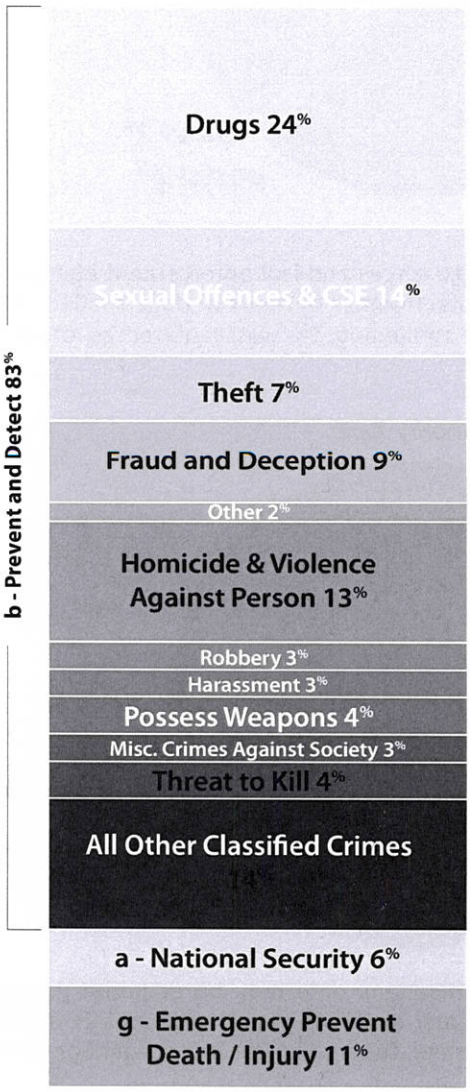


Urgent requests. Communications data may be acquired in exceptionally urgent circumstances through an oral application and approval. It might be the case, for example, that there is an immediate threat to life, or an urgent operational requirement,

with little or no time to complete the normal written process (see paragraphs 3.65-3.71 of the Code of Practice). In 2016, 10% of data requirements were approved orally under these urgency provisions.

Necessity statutory purpose. 83% of the items of data were acquired for the purpose of preventing or detecting crime or of preventing disorder. 11% were acquired for the purpose of preventing death or injury or damage to a person's mental health, or of mitigating any injury or damage to a person's physical or mental health. 6% were acquired in the interests of national security.

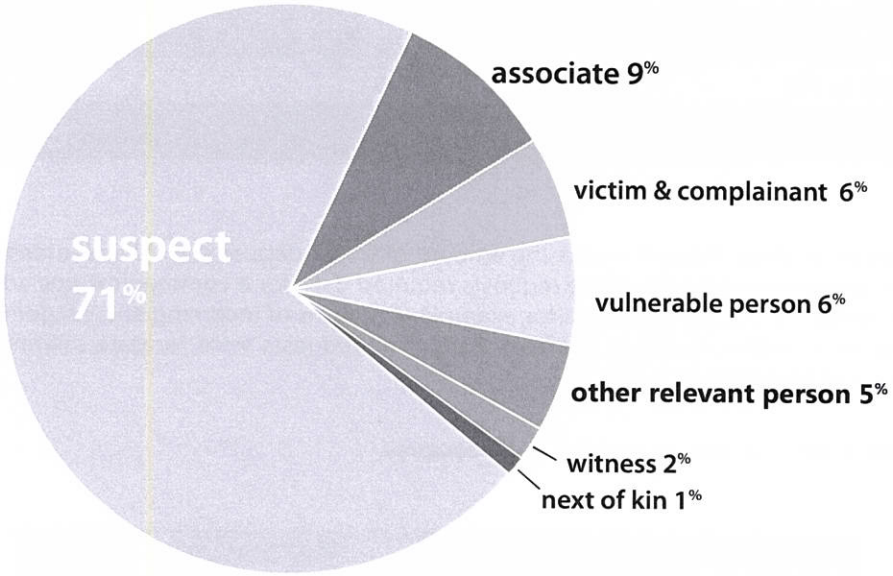
Figure 5 *Crime Type.*



Crime type. Figure 5 breaks down requests relating to criminal activity by crime type. Crime type statistics may be collected inconsistently, so this breakdown is indicative only.

Subject's relevance to the investigation. Public authorities record, for each item of communications data, whether that item of data relates to a victim, witness, complainant, suspect, next of kin, vulnerable person or other person relevant to an investigation or operation. **Figure 6** shows that 71% of requests were related to those suspected of committing crimes, or persons of interest to national security. 15% of requests were related to people who were not suspected of any nefarious activity.

Figure 6 *Items by subject's relevance to the investigation.*



Age of data requested. In terms of the age of the data requested, **Table B** shows the average age (in days). Public authorities have a significant demand for data that is less than one day old, with demand gradually falling from a few days old to a year or older. Approximately 70% of data requests were for data less than three months old, 25% aged between 3 months and 1 year, and 6% for data over 12 months old.

Table B *Items of Data by Age at the Point of Acquisition.*

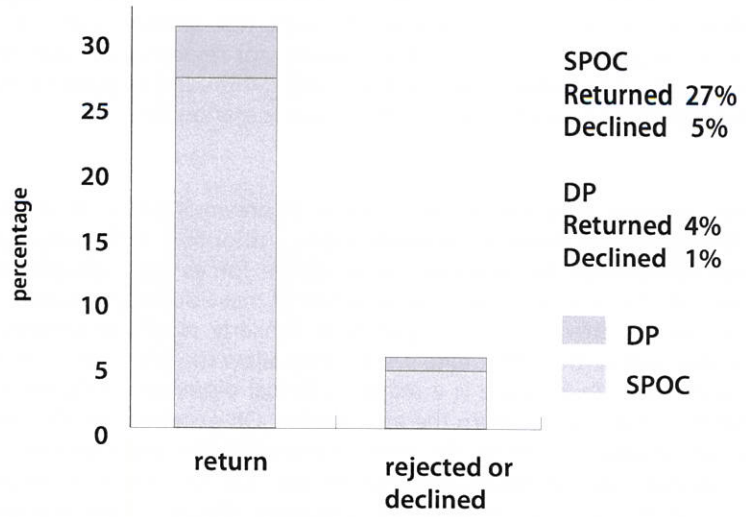
Less than a day	21%
1 to 7	9%
8 to 14	5%
15 to 30	10%
31 to 90	24%
91 to 120	7%
121 to 240	10%
241 to 365	8%
over 365	6%

Periods of data. Table C shows the amount of traffic data or service use information that was requested. 81% of the requests required data for a communications address for periods of 3 months or less (for example, 3 months of incoming and outgoing call data for a communications address). 25% of all requests were for data relating to a period of less than one day.

Table C *Items of data by period of data requested.*

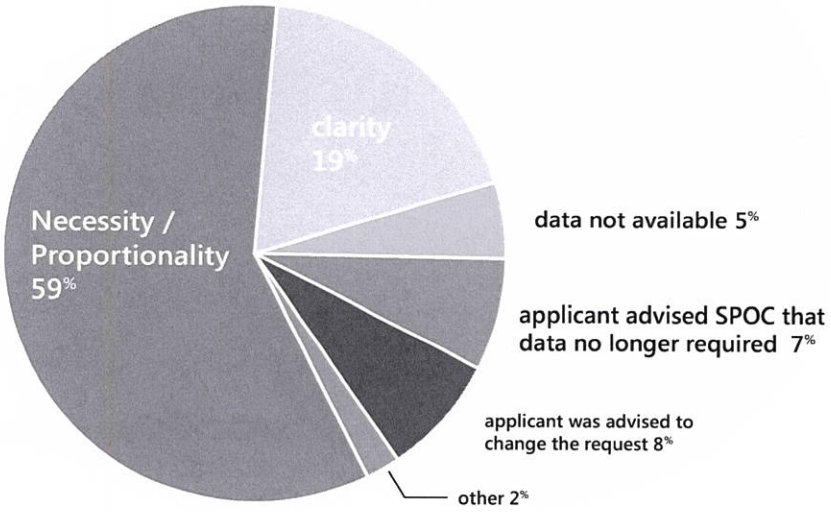
Period of data requested	Percentage
Less than 1 day	25%
1-7 days	15%
8-14 days	8%
15-30 days	13%
31-90 days	20%
91-120 days	6%
121-240 days	7%
241-365 days	3%
Over 365 days	3%

Figure 7 *SPOC and DP scrutiny.*



SPoC & DP scrutiny. 27% of submitted applications were returned to the applicant by the SPoC for development and a further 5% were declined by the SPoC (**Figure 7**). Reasons for refusing data applications included: lack of clarity; failure to link the crime to the communications address; and insufficient justification for collateral intrusion. 4% of submitted applications were returned to applicants by DPs for further development and 1% were rejected (**Figure 8**).

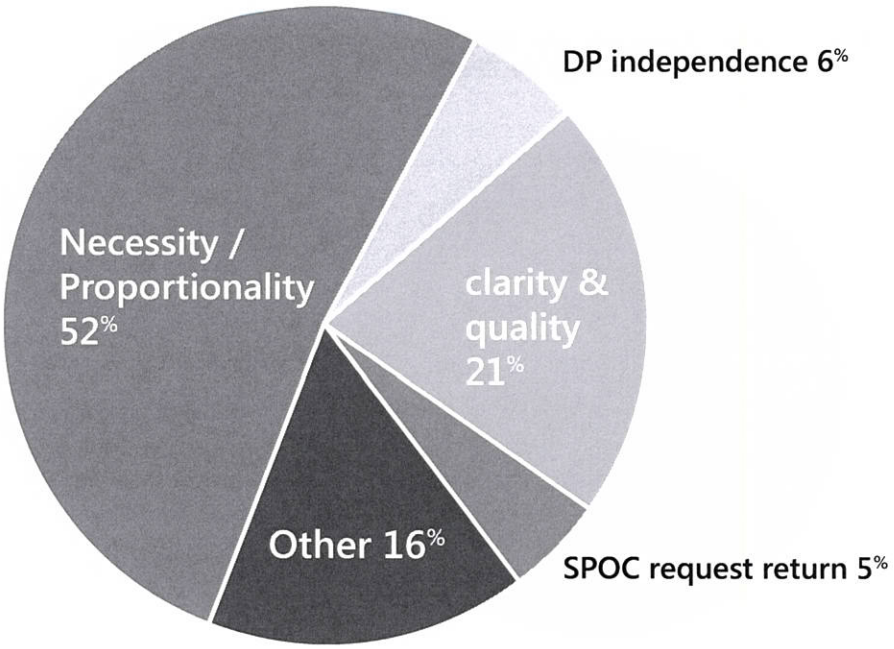
Figure 8 *breaks down the reasons why applications were returned for further development or declined by the SPoC.*



The main reason for DPs returning or rejecting applications (**Figure 9**) was that they were not satisfied with the necessity or proportionality justifications given (52%). A significant number of applications were returned because DPs were not satisfied with the overall quality or clarity of the application (21%). Other reasons for rejection included the DPs declaring that they were not independent of the investigation and requesting that the application be forwarded to an independent DP for consideration (6%).

These application rejection rates are similar to those of previous years. It remains the case that there is a significant variation between public authorities. Local practices may account for these differences; for example, some police forces have people drafting applications on behalf of investigators and the expertise of these dedicated people means that their applications are often of a higher standard. Similarly, workflow systems which are available to public authorities differ. One system may allow the SPoC officer to amend an applicant's submission where there is a minor technical discrepancy. Others do not, which means that the SPoC has to return the application. On occasion, IOCCO identifies high return rates which may, in part, be the result of a local policy which demands levels of technical knowledge beyond those required by the Act. On these occasions, my inspectors have reminded public authorities that applicants should merely *describe* what they require to meet operational objectives and that it is the role of the SPoC to *prescribe* the technical services which will meet those requirements.

Figure 9 *breaks down the reasons why applications were returned for further development or declined by the DP.*



Sensitive professions. The Code of Practice (paragraphs 3.72-3.77) requires applicants and DPs to give special consideration when considering applications for communications data which relate to persons who are members of professions which handle privileged or otherwise confidential information, for example lawyers or doctors. Public authorities must record the number of such applications and report to the Commissioner annually. In 2016, 47 public authorities advised that they had made a total of 948 applications that related to persons who were members of sensitive professions.

A significant proportion of these 948 applications were categorised incorrectly (i.e. the applicant had recorded a sensitive profession when there was not one). This was usually because the applicant erred on the side of caution, recording a sensitive profession if there was a possibility of one, rather than because they knew that there was one. This gives the impression of more requests for communications data relating to members of sensitive professions than have actually been made. It provides me with a greater level of assurance that DPs are taking sensitive professions into account when necessary.

Most applications relating to members of sensitive professions were submitted because the individual had been a victim of crime or was the suspect in a criminal investigation. In these cases, the profession of the individual was usually not relevant to the investigation, but public authorities showed proper consideration of the sensitive profession by bringing it to the attention of the authorising officer.

Inspection Regime

Communications data inspections are structured to ensure that the terms of Chapter 2 of Part 1 of RIPA and the associated Code of Practice are being properly followed. A typical inspection may include the following:

A review of recommendations from the previous inspection and progress towards their implementation.

An audit of the requests that public authorities have made to CSPs for the disclosure of data. This information is compared against the applications held by the SPoC in order to verify that approvals were given to acquire the data. This part of the process should also reveal whether any data disclosed by a CSP was not authorised.
The random examination of applications for communications data to assess whether the case for necessity and proportionality had been met.

An interrogation of the secure auditable computer systems used by larger public authorities to identify and analyse trends, patterns and compliance issues across large volumes of applications. For example, inspectors might use the system to show us every application which included the word 'journalist'.

The scrutiny of large-scale or otherwise significant investigations, for example investigations involving numerous IP address resolutions.

An examination of urgent oral approvals to confirm that the process was used appropriately.
A review of the errors reported or recorded, including checking any measures put in place to prevent recurrence.

Number of inspections. In 2016, my inspectors conducted 68 communications data inspections. These reviewed 52 police forces and law enforcement agencies, 3 intelligence agencies, and 13 'other' public authorities including the National Anti-Fraud Network (NAFN), which acts as the SPoC for all local authorities.

The length of an inspection depends on the type of body being inspected and its communications data usage. The inspections of larger users, such as police forces and intelligence agencies, are conducted by at least two inspectors and take place over 3 or 4 days. The inspections of smaller volume users can be conducted over a day by a single inspector.

Query-based searches. IOCCO works closely with the software companies that supply secure auditable systems for administering communications data applications for most police forces and law enforcement agencies. These systems can be searched to give better insight into the activities undertaken by the authorities. This enables specific areas to be tested for compliance and to identify trends, for example:
Records of authorisers' considerations enable inspectors to confirm that that they are discharging their statutory duties responsibly, that they are of the requisite seniority or rank and that they are independent of the investigation.

Applications for large amounts of communications data or for particularly intrusive datasets are tested to confirm that the requirements of necessity and proportionality have been applied appropriately.

Inspection Findings and Recommendations

Following the inspection, IOCCO publishes an inspection report setting out its findings and recommendations and giving a judgement on the overall level of compliance. These reports identify the level of compliance against a set of baselines, which are derived from Chapter 2 of Part 1 RIPA and the Code of Practice. When necessary, they contain recommendations with a requirement for the public authority to report back on progress against the implementation of remedial action.

The total number of recommendations made during the 68 communications data inspections in 2016 was 235. 55 public authorities received at least 1 recommendation. A traffic light system (red, amber, green) allows public authorities to prioritise remedial action:
Red recommendations are of immediate serious breaches or areas of non-compliance with the law or of the code of practice.
Amber recommendations identify where there has been non-compliance but to a lesser extent. Remedial action should prevent potential escalation to more serious breaches.
Green recommendations are issued where the public authority could act more efficiently or where better practices are available.

This year, 10 recommendations (4.3%) were red, 144 (61.3%) amber and 81 (34.4%) green.

The relative proportion of red, amber and green recommendations has remained broadly the same over recent years, although the specific public authorities inspected change each year. My previous annual report noted that there had been a slight rise in the average number of recommendations per public authority, from 4 to 5. This rise was attributed to difficulties in understanding or otherwise complying with the requirements in the revised Code of Practice regarding record-keeping, DP independence and applications relating to sensitive professions. This year, the average number of recommendations per public authority in 2016 reduced to fewer than 3.5 per authority. This may indicate that the requirements of the Code are being better understood and complied with.

At the end of each inspection, the authority is given an overall rating of good, satisfactory or poor, depending on an assessment of the total number and severity of recommendations made. Whether previous recommendations have been achieved is of particular relevance. In 2016, 61 public authorities achieved a 'good' rating. Seven were scored 'satisfactory'. No public authorities received a 'poor' rating. A list of public authorities' scores in communications data inspections can be found in Annex B.

Principal Recommendations and Key Issues

The most common subjects of recommendations are:

- Records and record-keeping compliance (46)
- Quality of applications (43)
- SPoC efficiency and effectiveness (27)
- DP's independence (24)
- DP's considerations (18)
- Sensitive professions (18)

Records and Record-keeping Compliance (46)
These recommendations are frequently the result of authorisations or statutory notices failing to contain the necessary content (see paragraphs 3.37 and 3.47 of the Code of Practice). Other occurrences include failures to maintain auditable records or to provide IOCCO with comprehensive or accurate statistical returns.

Quality of Applications (43)
Some applications failed to fully justify necessity or proportionality, in particular where:

- applicants did not account for the link between the communications address and their investigation;
- an incorrect statutory purpose had been specified in the application;
- it was unclear what specific crime type was being investigated;
- the likelihood of collateral intrusion had not been sufficiently considered; or
- the relevance of the date or time periods sought had not been justified.

SPoC Efficiency and Effectiveness (27)
The Code of Practice places responsibility on the SPoC to act as guardian and gatekeeper of the acquisition and disclosure process. Many of the recommendations in this category result from: failures adequately to advise applicants and DPs; unnecessarily returning applications which could legitimately be refined and progressed by the SPoC; and failures to identify key matters such as statutory purposes.

Designated Person's Independence (24)
Paragraph 3.12 of the Code of Practice states that DPs must be independent of operations and investigations when granting authorisations or giving notices related to those operations. Advice around DP independence changed in the March 2015 Code of Practice. As a consequence, 34 DP-independence-related recommendations were made in 2015. During the 2016 inspection programme, it was apparent that most public authorities have addressed the issue of DP independence, and so errors have reduced by almost a third.

Structural and procedural changes have been introduced across many authorities to ensure that DPs do not have line management responsibility for applicants or that their geographical and functional commands have no connection with the investigations or operations that are supported by the applications. The 24 recommendations, however, illustrate that some public authorities still need to fully implement this.

Designated Person's Considerations (18)
This category of recommendation focuses on the content of the DP's recorded considerations. Each application should receive bespoke consideration based on the unique elements of the crime or event under investigation. These recommendations address those DPs who make little reference to the specifics of the application in hand, using generic language.

Sensitive Professions (18)
The revised 2015 Code of Practice requires UK law enforcement agencies to seek judicial authorisation when applying for communications data to identify or to determine journalistic sources. Following some previous cases of poor compliance in this area, inspectors have issued recommendations to public authorities who have failed to address the relevance of the sensitive profession or where there might be unintended consequences of applying for such data.

Communications Data Errors

What is a communications data error?

Paragraphs 6.11 to 6.28 of the Acquisition and Disclosure of Communications Data Code of Practice explain the point at which errors occur and the actions required of the public authority or the Communication Service Provider (CSP).

An error may occur when a designated person:
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.

There are two categories of errors: reportable and recordable.

Recordable errors: When an error has occurred but is identified by the public authority or the CSP *without data being wrongly acquired or disclosed*, a record will be maintained by the public authority. The record will explain how the error occurred and provide an indication of steps taken to ensure that a similar error does not recur. Inspectors examine the recordable errors along with any steps the public authority has taken to prevent recurrence. An example of this category of error would be an incorrect transposition of information that does not result in the wrongful acquisition or disclosure of communications data, for example if an incorrectly typed phone number is invalid.

Reportable errors: A reportable error occurs when an error leads to communications data being acquired or disclosed. In some instances, wrongful disclosures infringe the rights of individuals unconnected with the particular investigation or operation. Reportable errors must be reported to my office within five working days of their being discovered (see paragraphs 6.15 and 6.19 of the Code). The error report must explain how the error occurred, indicate whether any unintended collateral intrusion has taken place, and provide an indication of the steps that have been or will be taken to ensure that a similar error does not recur. An example of a reportable error would be a case where an incorrectly typed phone number is valid, and information relating to it is disclosed to the public authority.

The vast majority of reportable errors are self-reported to my office by public authorities and CSPs. I am glad to record that there remains a very strong culture of self-reporting by both public authorities and CSPs.

Error Statistics

Usually one human mistake will result in one erroneous disclosure (e.g. an applicant submits a request for subscriber data on the wrong telephone number and erroneous subscriber details are acquired). However, when the error is caused by a technical system, for example a CSP's secure disclosure system, one error could well result in multiple erroneous disclosures.

Figure 10 *2016 Errors breakdown by Responsible Party and Cause.*

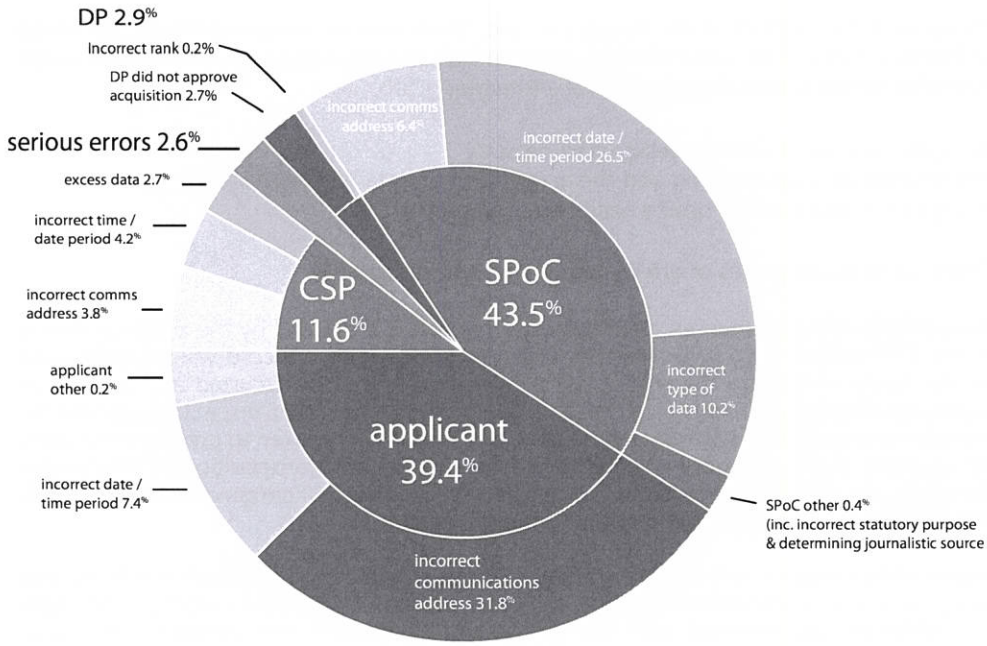


Figure 10 shows the breakdown of the 1,101 errors that occurred in 2016, by responsible party and cause. A comparison with the 2015 figures reveals that the biggest single cause of error remains the submission of incorrect communications addresses by applicants. SPoCs are responsible for 43.3% of errors. This is largely because of the complexity of their role, and the amount of manual typing that is still sometimes required of them.

Serious Error Investigations

Paragraph 6.22 of the Code 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 error on the affected individual's rights. The Commissioner may inform the affected individual and notify them of their right to make a complaint to the Investigatory Powers Tribunal.

This discretionary power supplements the Commissioner's duty in paragraph 8.3 of the Code. This requires the Commissioner to inform any individual who has been adversely affected by a wilful or reckless error.

I have 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 a 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 if, having failed to take account of an obvious and serious risk, there has been an adverse impact on an individual.

The circumstances in which an error would be classified as "serious" include:

- Technical errors relating to CSP secure disclosure systems, which result in a significant number of erroneous disclosures.
- 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 arrest of a person).
- Errors which result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

IOCCO's error investigation procedure determines whether any reportable error falls into one of the above categories. In some cases, there may be no direct adverse impact on any individual (for example, a technical system error which led to false negative results). In this case, an inspector would still investigate the error and ensure that measures are put in place to prevent any recurrence.

In cases where there was wilful or reckless conduct and an individual had been adversely affected, I would invoke my power under Paragraph 8.3. In cases where there was no wilful or reckless conduct, I would still consider using my discretionary power in Paragraph 6.22. I would assess the impact of the interference on the affected individual's rights and might decide to inform them of the error.
Importantly, under the Investigative Powers Act 2016, there will be a change in the thresholds regarding when the Investigatory Powers Commissioner can inform an individual. Section 231 of the Act requires the Commissioner to inform a person of any relevant error where they consider it is serious and in the public interest for that person to be informed. The Commissioner is not permitted to determine that a matter is serious unless they conclude that the error has caused significant prejudice or harm to the person concerned.

Whether this will have an impact on the numbers of persons being informed of serious errors is difficult to judge. Under the existing regime, all occasions on which I have notified individuals of an error were cases in which they had suffered significant prejudice or harm (such as being arrested) and so would be covered under the new Act.

In circumstances where a serious error is assessed to have occurred, an Inspector is allocated to investigate the cause of the error, the impact on the affected individuals' rights (if applicable) and the measures put in place to prevent recurrence. In cases where human error is identified, a timeline of events is prepared to establish how the error came about and any missed opportunities to identify it.
In the case of technical errors, the inspector works with the CSP and their vendors to discuss the cause and the measures put in place to remedy the issue. Potentially erroneous disclosures are checked and assessed. My office then contacts the relevant public authority to understand the impact that each disclosure may have had upon an individual

or investigation. The inspector ensures that any wrongly acquired data is deleted in line with paragraph 6.24 of the Code, or that any data obtained in excess of that which was authorised is managed appropriately (see paragraphs 6.26 to 6.28 of the Code).

Once the investigation has been concluded, I receive a detailed report setting out: a summary of the incident; a description of the circumstances leading to the error; the cause of the error; its impact; the measures put in place to prevent the error recurring; and any recommendations. Attached to this report will be advice from the Head of IOCCO and my legal adviser on any action I should take with respect to the error.

Summary of Serious Investigations

During 2016, IOCCO undertook 35 serious error investigations. I concluded that 6 of the 35 cases did not meet the serious error criteria.

The remaining 29 cases were classified as serious errors. Descriptions of these are set out in Annex D. 20 of these were human errors, 7 were system / workflow errors and in 2 instances communications data was obtained without the lawful authority. The impact of these errors was as follows:

- Persons unconnected to an investigation visited by police (9);
- Search warrant executed at an address of a person unconnected to the investigation and / or persons unconnected to the investigation arrested (7);
- Incorrect / missing / excess data (5);
- Delayed welfare check on vulnerable persons (5);
- Communications data acquired without lawful authority (2);
- Data obtained on individuals unconnected to an investigation (1).

Overall, the number of serious errors remains very low (0.004%). Human error still accounts for the majority of serious errors. Many of the most serious errors were caused by mistakes in the resolution of IP addresses. This is addressed in the next chapter.

IP Address Resolution Errors

I am concerned by the increasing number of errors that occur when public authorities try to resolve IP addresses. These have resulted in the wrong people being arrested for extremely serious crimes. I am devoting a chapter of my report to this issue in order to raise the profile of this issue within public authorities and among victims and their legal representation.

IP Address Resolutions

IP (Internet Protocol) addresses tell the internet where, physically, to send information. As a result, IP addresses can usually be used to link specific online activity to a specific physical device (i.e. a specific router or phone), which would often be linked to a specific location or individual. However, unlike a real physical address, the Communications Service Providers (CSPs) can easily reassign IP addresses, and it often makes sense for them to do so. For example, many CSPs have more customers than IP addresses, so they only assign IP addresses to active customers (those online). This means that when you log off, the IP address you were using is assigned to the next person. You may well have a different IP address when you log back in again. CSPs also sometimes change customers' IP addresses for security reasons. Changing your IP address makes it harder for 'cyber-criminals' to find you. More recently, CSPs have been routing multiple users through the same IP address. This saves on the number of IP addresses used but makes it hard to know which of those users is responsible for any activity coming through that address.

All of this means that turning an IP address into a specific location is increasingly complex. To link an IP address to a CSP's customer's address, the public authority needs to provide the time when online activity occurred. There is significant variation in how time is recorded online, in 'date stamps'. For example: 1 in the morning on the first of January 2017 could be represented as: 201701010100; 1.00 1-Jan-17; or 0100 1 January 2017. In addition, not all of these systems record the time zone.

Errors

All of this greatly increases the risk of error. Most of these are transcription errors (a number is typed in incorrectly). Based on the complexity set out above, it is easy to see why. But errors can also be caused by other issues. The impact of these errors has, in some cases, been enormous. People have been arrested for crimes relating to child sexual exploitation. Their children have been taken into care, and they have had to tell their employers. On confirmation of the error, all the power of the state, which comes into force to protect children, needs to be turned around and switched off. I have a great deal of admiration for Nigel Lang, who was arrested in error in these circumstances, for having had the courage to highlight this issue in the media.

By way of balance, it is worth highlighting that there is a reason why serious IP address resolution errors are relatively more common in relation to child sexual exploitation cases than other crimes. Public Authorities are understandably unwilling to take the risk of exposing children to paedophiles. As a result, where an IP address resolution shows a

property at which children are living, some of the usual investigative work, which would corroborate the resolution but takes time, is not always done before executive action is taken. There needs to be a change of mindset away from the assumption that technical intelligence, such as an IP address resolution, is always correct.

Many of the errors set out in Annex D are IP Address Resolution Errors.

IOCCO's response

Last year, I decided to review the measures that had been taken to improve processes, training and general awareness, with the intention of reducing these errors. In addition, I wrote to the National Police Chief's Council lead on communications data on 16 December 2016. During my review, inspectors paid particular attention to the recommendations in my July 2015 half-yearly report:

- Make it easier for applicants to be able to electronically transfer (i.e. copy/ paste) communications addresses and timestamps into their applications;
- Resolve more than one IP address relating to the same activity and compare results;
- Make it easier for those processing applications to check the source information on which an application is based;
- Those receiving from CSPs the results of a resolution should double-check all disclosures against the original requirements prior to taking action; and
- Investigators should undertake further research and intelligence checks to try to corroborate the result before executing warrants.

During this review, inspectors have in particular focused on staff within teams that regularly resolve IP addresses using timestamp conversions.

My inspectors have found a wide variation of capabilities available to applicants to transfer electronically (i.e. copy/paste) communications addresses (and relevant dates / times / time zones) into their applications. Some investigators use dual-screen terminals with access to all systems within an inter-connected desk-top environment. Others work on standalone systems that require members of staff to use approved USB sticks to transfer data. Other investigators are required to re-type communications addresses (and relevant dates / times / time zones) into their applications. There are often good reasons for the use of standalone systems, but requiring investigators to re-type a significant number of IP addresses greatly increases the risk of error.

Where there is more than one IP address related to the incident, or more than one date / time, I am satisfied that investigators will usually seek to resolve more than one to make a comparison.

My inspectors have concluded that it is now common practice for applicants to make available to those who process the applications (the SPoC) the source information on

which their application is based. This enables the SPoC to check that the applicant has provided the correct data, and consider whether they interpreted the original information correctly. In practice, applicants now include a digital copy of the source information or a screenshot when submitting applications. Without exception, inspectors found that SPoCs were undertaking timestamp conversions and asking colleagues to check their conversion.

The capability for SPoCs to be able to electronically transfer (i.e. copy/paste) the communications address and timestamp from the application to the CSP was less consistent. The majority of public authorities receiving information from CSPs are checking and double-checking against the original requirements to identify inputting errors.

Many of the investigators who contributed to my review provided us with examples of the research templates and guides that they use to undertake intelligence checks to try to corroborate a physical address before applying for a search warrant.

Investigators targeting child sexual exploitation talked about their use of the *"KIRAT process"* to assist them in assessing risk. The Kent Internet Risk Assessment Tool (KIRAT) was developed by Kent Police and is part of an EU project called Fighting International Internet Paedophilia (FIIP)[1] that focuses on targeting offenders and developing victim identification. The University of Liverpool[2] is part of an EU consortium contributing to the work and described KIRAT as follows:

"[KIRAT] is used to risk-assess people who view indecent images of children on the Internet, helping police to assess the level of risk posed by a suspect and the likelihood of that person becoming a contact offender - someone who commits sexual offences against children."

Some investigators are using both KIRAT and their internal 'research templates' as part of the build-up to determining what follow-up action, such as seeking a search warrant, may be appropriate. Inspectors concluded that KIRAT was not in common use, and several investigators interviewed who work in this field were not aware of the tool. As it represents current best practice, I encourage all forces to use it where appropriate.

Based on the review, I was satisfied that improvements have been achieved in this area of work. In addition, in response to my letter, the police have created the Internet Protocol Address Resolution (IPAR) Best Practice Group. This is welcome. Based on best practice from around the country, the Group has already published three excellent guides. Each guide sets out a series of standards required of police officers. I have been pleased to note that during recent inspections, my inspectors have seen evidence of public authorities using these guides.

However, errors are still occurring, in part due to lack of awareness of the availability of

1 https://www.insight-centre.org/content/fiip-fighting-international-internet-paedophilia

2 https://www.liverpool.ac.uk/research/news/articles/researchers-and-police-receive-eu-funding-to-aid-child-protection-efforts/

systems and other processes that will help avoid them. Ultimately, there remains every likelihood that more innocent people will suffer a catastrophic event similar to Mr Lang's experience. In my speech at the International Communications Data and Digital Forensics Conference in March 2017, I put public authorities on notice that I am unhappy about the number of these errors, and that I would have no hesitation in using my powers of notification to enable victims to make applications to the Investigatory Powers Tribunal.

Bulk Communications Data

Background

The Prime Minster wrote to the then Commissioner in January 2015 to ask him to extend his oversight to include directions given by a Secretary of State under section 94 of the Telecommunications Act 1984. It was acknowledged that the Commissioner had previously provided *limited* non-statutory oversight of the use made of one particular set of directions by the Security Service. The Prime Minister was keen to extend that oversight to cover all use of the power.

In October 2015, IOCCO began its first review of directions issued under section 94 of the Telecommunications Act 1984. The purpose of the review was to identify the extent to which the intelligence agencies use section 94 directions, to assess what a comprehensive oversight and audit function of section 94 directions would look like, and to assess whether the systems and procedures in place for section 94 directions were sufficient to comply with legislation and any relevant policies.

On 4 November 2015, the Home Secretary made a statement in the House of Commons[3] about the then draft Investigatory Powers Bill:

"I have announced today our intention to ensure that the powers available to law enforcement and the agencies are clear for everyone to understand. [...] There remain, however, some powers that successive Governments have considered too sensitive to disclose, for fear of revealing capabilities to those who mean us harm. I am clear that we must now reconcile that with our ambition to deliver greater openness and transparency.

"The Bill will make

Public Electronic Communications Network

A public electronic communications network (PECN) is defined in section 151 of the Communications Act (2003) as:

"an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public."

This excludes those who provide services or networks that are not available to members of the public (typically, private networks and other bespoke services). PECNs tend to be bodies which would be referred to as CSPs under RIPA and in other parts of this report.

Bulk Communications Data

The term *bulk communications data* is explained in a Government paper entitled the *"Operational Case for Bulk Powers"*.[7] This was published to inform the public about provisions in what is now the Investigatory Powers Act 2016. It sets out the Government's explanation of what this data is, which agency may acquire it, and the reasons why and how it is used by the agencies when carrying out their statutory functions. The publication also contains several case studies provided by the intelligence agencies.

In simple terms, the use of section 94 directions has enabled the agencies to obtain communications data (all information relating to a communication except its content) in bulk. Bulk communications data involves large amounts of communications data, most of which relates to individuals who are unlikely to be of any intelligence interest.

Shortly after the publication of the review report, the then Independent Reviewer of Terrorism Legislation (David Anderson Q.C.) published his Review of Bulk Powers Report[8] in August 2016. He concluded:

"This Report has declared the powers under review to have a clear operational purpose. But like an old-fashioned snapshot, it will fade in time. The world is changing with great speed, and new questions will arise about the exercise, utility and intrusiveness of these strong capabilities. If adopted, my recommendations will enable those questions to be answered by a strong oversight body on a properly informed basis."

Update to my review report

IOCCO's review of directions issued under section 94 of the Telecommunications Act 1984

7 See section 9 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

8 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

made 9 recommendations.[9] My office has received full cooperation from the Security Service and GCHQ in their responses to the report's recommendations.

In the review report, I indicated that IOCCO would, on an annual basis, carry out formal inspections within any public authorities for which the Secretary of State has given section 94 directions for the acquisition of communications data. It remains the case that those are only the Security Service and GCHQ. More recently, they have agreed that inspections should be undertaken at least every 6 months with additional, on-going updates and discussion regarding the use of these powers.

The Investigatory Powers Act 2016[10] received Royal Assent in late 2016, and a draft code of practice relating to the bulk acquisition of communications data, pursuant to Schedule 7 was published in February 2017.[11] Once enacted, the IPA will place oversight of the acquisition of bulk communications data on a statutory footing.

Applications for section 94 directions

In the absence of any codified procedures in or made pursuant to section 94 of the Telecommunications Act 1984, the intelligence agencies developed a process to facilitate the acquisition of bulk communications data. That process is set out in the handling arrangements[12] published by the agencies in November 2015.

The process can be broken down into four distinct areas, some of which may be undertaken simultaneously:

a) The agency identifies and describes the bulk communications data considered necessary to meet its operational objectives;

b) The agency identifies the relevant PECN(s) and consults them to assess whether the proposed acquisition of data is reasonably practical or whether the specific data required could be separated more readily from other data;

c) The agency consults further with the PECN and assesses whether the data can be made available by means of a section 94 direction; and

d) The agency determines whether the bulk acquisition of communications data is appropriate under a section 94 direction. If so, the agency will prepare a detailed submission for consideration by the Secretary of State.

9 See Pages 54 & 55 http://iocco-uk.info/docs/56208%20HC33%20WEB.pdf

10 See http://www.legislation.gov.uk/ukpga/2016/25/part/6/chapter/2/enacted and sections 158 through to 175

11 See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593750/IP_Act_-_Draft_BCD_code_of_practice_Feb2017_FINAL_WEB.pdf

12 See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

Recent inspections of the Security Service and GCHQ sought to assess the progress made in relation to the recommendations included in the review report[13] and in relation to the draft code of practice.[14] In relation to current practice, my inspectors have concluded:

a) The Security Service and GCHQ each keep a central record of section 94 directions given by the Home Secretary or Foreign Secretary, respectively, on their behalf. The central record includes the date when the direction was given; the name of the Secretary of State giving the direction; the PECN to which the direction relates; a description of the conduct required to be undertaken and the date when the direction was served on the PECN. These records have been made available for inspection by IOCCO. This addresses Recommendation 1 in the review report.

b) A process is in place which allows for the secure electronic transfer of copies to IOCCO, from the Security Service and GCHQ, of section 94 directions given by a Secretary of State. This addresses Recommendation 2 in the review report.

c) Section 94 directions for bulk communications data now indicate the specific communications data that is required to be disclosed by the PECN. This addresses Recommendation 3 in the review report.

d) An application process has been developed that accounts for the requirements of the Investigatory Powers Act 2016. This addresses Recommendation 4 in the review report.

e) The Security Service and GCHQ undertake reviews every 6 months as to whether the acquisition of bulk communications data remains necessary and proportionate. The results of these reviews, and their recommendation to keep the direction in place, modify or cease its use are submitted to the Secretary of State. This addresses Recommendation 6 in the review report.

f) There is a mature process in place for the reporting of errors. This mirrors the processes for reporting other errors to IOCCO.

g) All existing directions were replaced by new directions in October 2016 as a consequence of the recommendations.

Access to the bulk communications data retained by the agency

Recent inspections of the Security Service and GCHQ examined the procedures in place to access data for operational purposes. My inspectors interviewed those in charge of intelligence operations, senior managers authorising access, analysts within operational teams and those who undertake internal audits.

13 See Page 54 & 55 http://iocco-uk.info/docs/56208%20HC33%20WEB.pdf

14 See footnote of this report

Interception warrants have to be authorised personally by a Secretary of State (sections 5(1) and 7(1)(a)). They must sign the warrant personally, or in urgent cases verbally authorise the issue of a warrant signed by a senior official (section 7(1)(b)).

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

- the Defence Secretary;
- the Foreign and Commonwealth Secretary;
- the Home Secretary;
- the Secretary of State for Northern Ireland; and
- the Cabinet Secretary for Justice for Scotland[22].

Statutory 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;[23]
- for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security,[24] 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)).

These statutory purposes are taken directly from Article 8 of the European Convention on Human Rights. To issue an interception warrant for any other purpose would be unlawful. It is part of my function to ensure that all warrants are issued for these statutory purposes only.

Proportionality. The Secretary of State may not issue an interception warrant unless they believe that the conduct authorised by the warrant is *proportionate* to what is sought to be achieved by that conduct.

Proportionality is an important principle in human rights jurisprudence that runs throughout RIPA and its application. Every application for an interception warrant must explicitly address necessity and proportionality. Secretaries of State have to address proportionality when deciding whether to issue an interception warrant. In considering proportionality, the

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

23 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.

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

and their related communications data; and

- the Secretary of State gives a *certificate* describing 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).

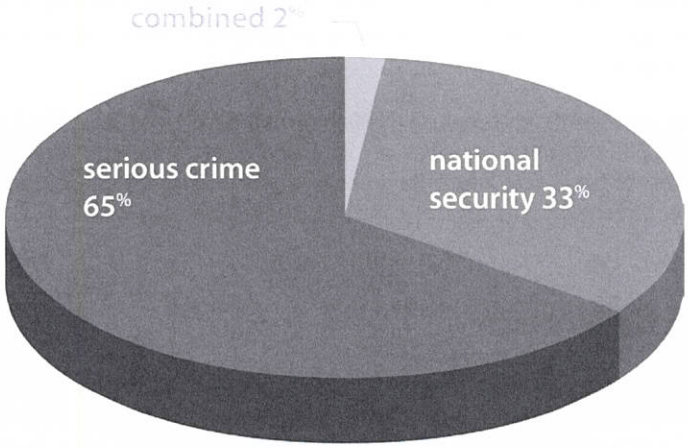
By virtue of section 8(5)(b), an interception warrant may also authorise other conduct as described in section 5(6). Such conduct includes the interception of communications not identified in the warrant, the interception of which is necessary in order to do what the warrant expressly authorises. Therefore, a section 8(4) warrant can authorise the interception of communications which are not external communications to the extent that 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 the wanted external communications.

A section 8(4) warrant should contain the details required by paragraph 6.10 of the Interception of Communications 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 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) necessary 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)-16(6) of RIPA; and
- an assurance that all intercepted material will be handled in accordance with the safeguards required by section 15 and 16 of RIPA.

Figure 12 *details the breakdown of the 3,007 interception warrants issued in 2016 by statutory purpose.*



The combination category in **Figure 12** 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.

67 of the 3,007 warrants (approximately 2.2%) were approved urgently by the Secretary of State under the hand of a Senior Official after consultation with the Secretary of State. These warrants all related to exceptionally urgent cases where, for example, there was an imminent threat to life; an imminent threat to national security; a unique opportunity to obtain 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 National Crime Agency.

A Secretary of State refused an interception warrant on 5 occasions in 2016. The Government would argue that this figure is so low because of the high level of scrutiny that is applied to each warrant application before it is submitted to a Secretary of State. Any interception warrant is scrutinised by a number of people in the interception agency and the relevant warrant-granting department before it reaches the Secretary of State. This year, I asked the interception agencies and warrant-granting 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 10 occasions, the Senior Official or Secretary of State called for further information prior to approving a warrant.

These figures do not capture the critical quality assurance function initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department. Based on my inspections, I am confident that the low number of rejections reflects the careful consideration given to the use of these powers. Indeed, it is not uncommon to find intercepting agencies making conservative assumptions about what a Secretary of State is likely to approve.

The total number of warrants in force on 31 December 2016 was 1,602 – a 5.5% increase on 2015. Of the 1,602 warrants in force on 31 December 2016, 13 were issued under section 8(4). Some of the 1,602 warrants were first authorised before 2016 but the vast majority of interception warrants do not run for longer than six months.

Inspection Regime

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 for the Interception of Communications. Whereas many communications data inspections are carried out by my inspectors, I participate directly in nearly all interception inspections

After each inspection, my inspectors write a detailed inspection report and action plan stating the findings and recommendations. This is sent to the head of the interception agency and is copied to the relevant Secretary of State and warrant-granting department. Inspections of the four main warrant-granting departments are slightly different from inspections of the intercepting agencies. The warrant-granting departments are a source of independent advice to the Secretary of State and perform important pre-authorisation scrutiny of warrant applications and renewals to ensure that they are (and remain) necessary and proportionate. The emphasis during the warrant-granting 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 officials. After each inspection of a warrant-granting department, my inspectors compile a detailed inspection report and action plan stating the findings and recommendations. This is sent to the relevant Secretary of State.

Inspection Reports. After each inspection, my inspectors produce a report. In general, these will include:

- an assessment of how far the recommendations from the previous inspection have been achieved;
- a summary of the number and type of interception documents selected for 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 my office during the inspection period;
- an account of the examination of the retention, storage and destruction procedures;
- an account of other policy or operational issues which the agency or warrant-granting departments raised 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. I require the interception agency or warrant-granting department to inform IOCCO within two months of what progress has been made against these; and
- an overall assessment of the interception agency's or warrant-granting department's level of compliance with RIPA.

Number of inspections. In 2016, IOCCO moved from a biannual inspection regime to an annual one. I now inspect all nine interception agencies once and the four main warrant-granting departments twice. This, together with extra visits to GCHQ, made a total of **22** inspection visits last year. In addition, I and my inspectors arrange other ad hoc visits to agencies. As a point of principle, I inspect each warrant-granting 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-granting departments. In addition to the annual inspections, there are a number of additional visits and a large amount of correspondence throughout the year.

I usually recommend that public authorities retain warrantry for up to 2 years after the individual interception warrant has been cancelled to aid IOCCO inspections. However, it is also important to ensure that documentation is retained for a sufficient period to enable the Investigatory Powers Tribunal (IPT) to exercise its jurisdiction. Section 67(5) of RIPA provides that the IPT shall not consider or determine any complaint more than one year after the offending conduct has been carried out, 'unless it is equitable to do so'. It would be helpful if the Code of Practice for the new Investigatory Powers Act (IPA) clarified these matters and provided clear guidance.

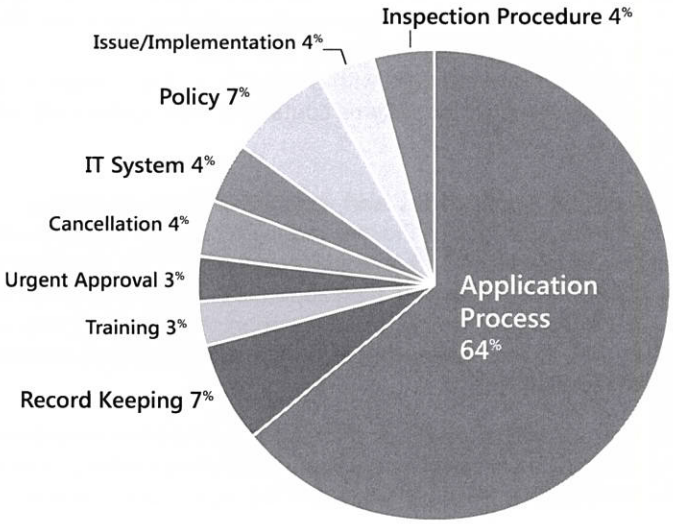
Inspection Recommendations and Observations

My inspectors made a total of 28 recommendations in their inspection reports. 14 were for the interception agencies and 14 for the warrant-granting departments. 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.

Application Process

18 of the 28 recommendations were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality and/or collateral intrusion justifications in the applications; or the handling of legally privileged or otherwise confidential material relating to sensitive professions.

Figure 13 *shows that the majority of the recommendations related to the application process.*



Necessity, proportionality and collateral intrusion
In some of the renewal applications, noted that the original assessment on collateral intrusion had not been reassessed following the addition of new communications addresses. My inspectors made a number of recommendations in this respect.

Legal professional privilege material and other confidential material
There are special arrangements and safeguards in the Code of Practice relating to communications involving legal professional privilege or confidential journalistic or personal material, which may give rise to issues under Article 6 (right to a fair trial) and Article 10 (freedom of expression) of the European Convention on Human Rights (ECHR), as well as Article 8 (right to privacy).

The recommendations reminded the intercepting authorities that renewals need to include 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 my inspectors' attention. They also recommended that managers should carry out regular reviews of intercepted material in order to ensure compliance with the safeguards.

Application templates. I favour a national application template to enable greater consistency in standards across the nine interception agencies. Further work has been done on this by agencies and warrant-granting departments in preparation for the implementation of the provisions in the Investigatory Powers Act. This will be a great help to judicial commissioners when they consider applications under the new Act.

Thematic warrants. I have had concerns about the scope of some thematic warrants, and how authorities were interpreting the definition of person as defined in 81(1) of RIPA, which states that a "person" includes any organisation and any association or combination of persons. As a result, some warrants were cancelled and in some cases new warrants were taken out against individuals rather than groups of people.

Changes to the GCHQ interception inspection regime

The last IOCCO annual report described a new 5-phase inspection regime for GCHQ, and stated that I would report back on how this had worked in practice.

Phase 1: Inspectors examined the warrantry applications by making selections at reading days and having further discussions on the inspection day with case officers from the relevant area.

Phase 2: Inspectors carried out an audit of a geographical area and were able to examine the necessity and proportionality statements made by analysts when adding a selector to the collection system for examination. Each statement had to stand on its own and had to refer to the overall requirement of priorities for intelligence collection. I was impressed by the quality of the statements.

Phase 3: GCHQ updated IOCCO on the retention, storage and deletion arrangements for systems containing intercepted material and related communications data. I also received additional briefings on the various collection systems.

Phase 4: GCHQ provided comprehensive details of the sharing arrangements whereby Five Eyes partners can access elements of the product of GCHQ's interception warrants on their own systems. My inspectors also met representatives of the Five Eyes community and received a demonstration of how other Five Eyes members can request access to GCHQ's data. Access to GCHQ systems is tightly controlled and has to be justified in accordance with the laws of the host country and handling instructions of section 15/16 safeguards. Before getting any access to GCHQ data, Five Eyes analysts must complete the same legalities training as GCHQ staff.

Phase 5. My inspectors met GCHQ and other agency staff on several occasions to clarify what constitutes an error and the timescales in which errors should be reported. I hope that the new Code of Practice for the Investigatory Powers Act will provide clarity in this respect. GCHQ now has more resources in this area and has cleared its error backlog. GCHQ errors tend to be caused by technical rather than human error.

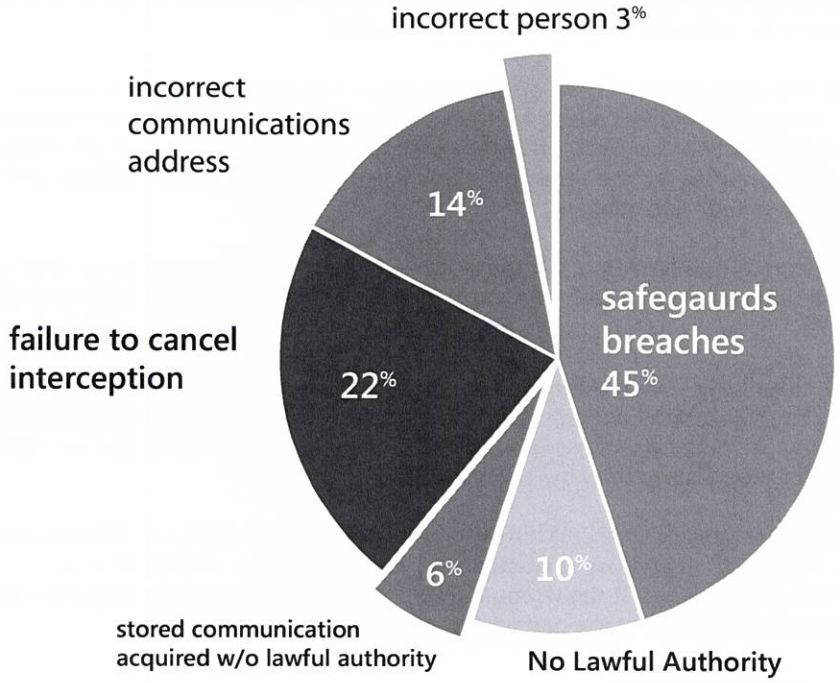
Interception Errors

Error reporting is an important part of the oversight regime. It is vital to ensure a consistency of approach from all interception agencies in terms of the thresholds, judgments and reporting criterion for errors. I welcome efforts in the Investigatory Powers Bill and the draft Code of Practice for the Interception of Communications to define an error and to introduce error reporting procedures.

Error statistics

The total number of interception errors reported to IOCCO during 2016 was 108 – a marked increase on the previous year's total of 68. The increase can be partly explained by the clearing of a backlog of previous errors by GCHQ. The breakdown of the causes of the errors is contained in **Figure 14.**

Figure 14 *Breakdown of the causes of interception errors.*



Descriptions of the key causes of interception errors are set out below.

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 wide-ranging consequences (i.e. large volumes of material erroneously collected). In some of these cases, the material and data contained details of individuals' private communications.

These errors can take a number of months to investigate. Happily, the cause of the error or systems malfunction is usually identified and completely resolved. A significant amount of work is undertaken to implement measures to prevent recurrence. In some cases, periodic sampling and checking procedures have been introduced to enhance agencies' ability to monitor and detect such errors. In all cases, the erroneous material and data is deleted.

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 United Kingdom; or technical failures which led to the incorrect selection of material or material continuing to be collected after it had been de-tasked.

Incorrect dissemination. These errors constitute non-compliance with section 15(2) of RIPA. They were mainly caused by the misdirecting of the intercepted material and related communications data to the incorrect interception agency. In all cases, the mistake was identified by the receiving agency immediately and the material and data received erroneously was deleted.

Failure to cancel interception. These errors were in the main caused by staff in the interception agency, warrant-granting department or CSP failing to effect the cancellation properly.

Incorrect communications address intercepted. Some errors were the result of the incorrect communications address being intercepted. The majority of these errors are human in nature, such as transcription errors, although some were due to technical systems failing to update correctly.

Incorrect person Intercepted. Whilst similar to the incorrect communications address category above, this category includes instances where the interception agency has applied for a warrant against the wrong number, or is otherwise conducting interception against someone who is not the correct target. This can be because of:

- technical reasons;
- the phone belonged to someone other than the subject of interest; or
- the communications device had been handed over to a third party.

In most of these cases, the intercepting agency had a strong case to assess that the user of the phone would be the intended target, and is not at fault for the error. The analysts

processing the interception product detected these errors promptly and the interception was immediately suspended and then cancelled. It is important that agencies report such instances to IOCCO. Even though the interception of the communications address was authorised by the Secretary of State, the conduct resulted in intrusion into the privacy of individuals who were not of intelligence interest and for whom the Secretary of State did not consider the necessity or proportionality of such measures. As a result, I do not consider the interception to have been properly authorised. The agencies must take steps to reinforce within operational teams the importance of identifying promptly when a subject of interest is not using a particular communications address, ensuring that the interception is suspended and cancelled immediately.

The interception agencies, warrant-granting departments and CSPs provided IOCCO with full reports of the errors. I am content 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.

Prisons

This section outlines the legislation governing the interception of prisoners' communications and summarises the key findings from our IOCCO's 2016 prison inspections.

Overview

The Interception of Communications Commissioner's non-statutory oversight of the interception of communications in prisons within England and Wales commenced in 2002. It was expanded to include Northern Ireland in 2008. IOCCO does not, currently, provide oversight of interception within Scottish prisons. In the near future, the inspection of all prisons in the United Kingdom, in relation to their use of investigatory powers, will be placed on a statutory footing by the Investigatory Powers Act.

The inspections of prisons carried out by my inspectors are based on Prison Rules and Prison Service Instructions (PSIs). Prison Rule 35A gives any prison Governor the authority to intercept any communications by any prisoner or class of prisoners, subject to necessity and proportionality. Prison Rule 81 also gives a Governor the ability to delegate the powers given to him by the rules to another officer of that prison. In practice, the responsibility to consider and authorise requests to intercept prisoners' communications is normally delegated to the Head of Offender Management team or the Head of Prison Security.

In July 2016, Her Majesty's Prison & Probation Service (HMPPS) issued an updated Prison Service Instruction called 'The Interception of Communications in Prisons and Security Measures'. This introduced a number of improvements to the management of communications interception in prisons. These included:

- Implementing a new Interception risk assessment / application process.
- Introducing electronic monitoring documents.
- Introducing a structured management and supervision process.

It was apparent from the inspections conducted after July 2016 that a number of prisons found it challenging to implement the new Instruction. Prisons officers did not always understand the new measures, and did not appear to be resourced to implement them. As a result, my inspectors have frequently been asked to provide guidance on the implementation of the measures, inspection scores have been weaker, and inspectors have issued more recommendations.

Inspections and Recommendations

The objective of an inspection is to ensure that:

- all prisons are fully discharging their responsibilities to inform the prisoners that their communications may be subject to interception;
- all prisoners are aware that confidential communications such as calls to lawyers and confidential access organisations such as the Samaritans should not be intercepted;

- the correct authorisations and risk assessments are in place to support the monitoring of prisoners' communications;
- all interception is carried out lawfully and in accordance with the Human Rights Act (HRA);
- there is consistency in the approach to interception; and
- appropriate measures are being afforded for the retention, storage and destruction of intercept product.

In 2016, my office conducted 76 prison inspections. The majority were conducted in a single day. The total number of recommendations made was 418 – an average of 5.5 recommendations for each prison. These recommendations are given a 'traffic light' rating, in line with the standard practice across IOCCO inspections.

In 2016, 19% of the recommendations were red, 62% amber and 19% green. Prisons received the following overall grading:

- 65% received a good grade
- 20% were satisfactory
- 15% were poor.

A full list of prisons inspected and their scores can be found in Annex C.

Prisoners' telephone calls are controlled by a pin-phone system. Each prisoner has an individual telephone account, which is accessed by their pin-number. Prisons discharge their responsibility to inform prisoners that communications may be intercepted by issuing, on arrival, a communications compact. This document informs prisoners of the interception process, confidential calls and the statutory purposes for which a Governor can authorise interception.

The administration and content of the communications compact were amended by the 2016 Instruction. This caused some confusion, and a number of recommendations were made to correct problems where:

- staff were issuing old versions of the compact;
- copies were not being supplied to prisoners;
- documents were unsigned;
- compacts had been stored or disseminated incorrectly; and
- there was poor provision for prisoners with language difficulties.

When a communications compact is served, prisoners individually request the authorisation of their pin-phone contacts. In all of the establishments inspected, this process was in order and completed to a good standard. However, some prisons were vulnerable to abuse by prisoners who had made requests for numbers to be placed on the secure side of the system in an attempt to prevent their communications being intercepted rather

than because those numbers genuinely should not have been intercepted.
If a request to intercept a prisoner's communications is made on the grounds of public safety or to maintain prison security, there needs to be an Interception Risk Assessment. This should explain the threat, provide a proposed course of action, and justify the proportionality. However, my inspectors frequently found that that these necessity and proportionality justifications were not detailed or strong enough to enable the prison to demonstrate how a Governor had made an informed decision whether to intercept that prisoner's communications. This was particularly frequent in assessments, authorisations and reviews of prisoners who pose a risk to the public, such as those convicted of a sexual offence.

Since the introduction of the new Instruction in July 2016, 38% of establishments have failed to complete the application process to a suitable standard. Inspectors highlighted:

- incorrect documentation;
- a general lack of detail;
- lack of Human Rights justifications;
- no considerations by an authorising officer and
- poor reviews

In addressing this key area of the process, I endorse the comments made by my predecessor Sir Swinton Thomas during his first inspection of HMP Belmarsh in November 2002:

'I consider that there is an urgent need for all those engaged in this work to be provided with a written document detailing the safeguards that must be followed in relation to the interception of prisoners' communications of a type which is familiar to those engaged in interception work in law enforcement and intelligence fields. There is also a need for those engaged in this work to be trained as to their obligations. This appears to be notably absent at the present time. I am confident that this is not a problem that is peculiar to this prison and needs to be addressed by the Prison Service.'

In 44% of cases, prisons were not listening to all relevant intercepted calls in a timely manner. This is a concern. Either prisons are taking a risk by failing to conduct interceptions they have identified as necessary for safety reasons, or the original cases were incorrect and the prisoners in question should not have been intercepted at all.

To improve standards in interception and to ensure that risks are managed correctly, the 2016 instruction recommended a Daily Management log. This electronic document was designed to summarise the intelligence gathered on a daily basis on each prisoner subject interception. It should act as an overarching management tool to support staff and raise the profile of interception. However, use of the Daily Management Log required a computer to be located next to the pin-phone monitoring terminal. Many prisons had not installed a new computer, and so, between July and December 2016, only 22% met this new requirement.

Another amendment required the physical recording of all forms of interception to be completed electronically. In similar circumstances to the Daily Management Log, only 22% of

establishments had implemented a suitable electronic system; the remaining 78% continued to rely on paper records. In many cases, these were poorly completed, and in some cases illegible. I am now aware that a number of prisons have requested new IT equipment to implement this requirement, and so I expect to see better performance in 2017.

Considerable improvements have been made in the storage and destruction of intercepted material over the last few years. The majority of prisons have installed an automated deletion program, which deletes all pin-phone communication after a 3-month retention period. Compliance in this area is very good and no significant recommendations were made.

A recent priority for many prisons has been preventing the supply and possession of synthetic drugs. This has resulted in an increase in the interception of incoming mail and especially in letters fraudulently claiming to contain legal or confidential documents. Despite the increase in volume, this process is well managed. No recommendations were made in relation to this aspect of interception.

The Investigatory Powers Act

The Investigatory Powers Act received Royal Assent on 29 November 2016. It will come into practice through a series of commencement orders throughout 2017 and 2018. Previous reports set out IOCCO's engagement with the Government, Parliamentarians and civil society during the passage of the Bill. Here I will set out the major changes to the law governing the interception of communications, and consider how much of the 'IOCCO wish-list' made it into the final legislation.

The Act abolishes my office of Interception of Communications Commissioner. It also abolishes the Intelligence Services and Surveillance Commissioners. My functions will be carried out by the Investigatory Powers Commissioner and his Judicial Commissioners. Combining oversight powers and offices in this way should improve the quality and consistency of oversight. My oversight of prisons, which has previously been on a non-statutory basis, will be carried out on a statutory basis by the Investigatory Powers Commissioner.

The most significant change in the Act is the introduction of the judicial 'double lock'. For certain investigatory techniques, in addition to existing authorisation processes, it will be necessary for one of the judicial commissioners to also consider the application, and to decide whether to approve it. With respect to the interception of communications, this process will apply to interception warrants, bulk interception warrants, warrants authorising the bulk acquisition of communications data, and technical capability notices. In terms of volume, the overwhelming majority of these applications will be for lawful interception relating to a single target of interception (for example, a serious criminal). The bulk warrants and technical capability notices will be much less common but far more complex. Warrant requesting departments will need to give commissioners enough time to properly consider the technical and privacy implications of these applications and the Commissioner's office will need to include enough expertise to advise on these issues.

My office engaged proactively with a wide range of stakeholders, in Government, Parliament and civil society, during the passage of the Act. Of the six items on the IOCCO 'wish-list', three have been fulfilled in full. The new Commissioner will expect their inspectors to have increased access to technical systems; there is provision for the new Commissioner to launch their own investigations and currently a plan to have a small team conducting them; and the additional skills I wanted to see in the new body (technical, legal and communications) should be present in various forms.

Three wishes have not been fulfilled. The first was that the Act should relax secrecy provisions to aid transparency. There is a provision for the Commissioner to make disclosures in certain circumstances, but no general commitment to transparency within the Act. This is partly a question of culture. In my view, the new Commissioner should aim to continually push the boundaries of what information can be communicated to the public about the activities of its intelligence and law enforcement agencies.

I also wanted the rules around error reporting to be clearer, and to give the Commissioner greater powers to notify individuals who have been the victim of an error (so-called 'notifications'). Section 231 of the Act specifies that notifications can only occur where 'an error has caused significant prejudice or harm to the person concerned. Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning

of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.' It will be interesting to see how the Commissioners interprets this in practice.

While my wish for a single public-facing oversight body has been fulfilled, my wish that this should be a 'Commission' has not. This means that the Investigatory Powers Commissioner's Officer (IPCO) will be staffed by Home Office civil servants, with the Chief Executive managed by a Home Office Director. This raises questions around independence. In addition, I felt that the creation of a Commission would give the Commissioner's staff more powers to request access to information and systems. This is important to enable rigorous inspections, which will continue to be carried out, in the majority of cases, by civil servant inspectors rather than judicial commissioners. I recommend that consideration be given to using the provision under 238(5) of the Act to delegate statutory powers of inspection to inspectors.

Annex A: Number of Communications Data requests by public authority

The Intelligence Services

	Total Items of Data
GCHQ	4156
MI5 - Non S.94	39364
SIS	453

Police and Law Enforcement Agencies

	Total items of data
Avon & Somerset Constabulary	13160
British Transport Police	2404
Cambridgeshire & Bedfordshire Constabulary	9433
Cheshire Constabulary	10761
City of London Police	4472
Cleveland Police	6861
Cumbria Constabulary	3625
Derbyshire Constabulary	5588
Devon & Cornwall Police	18300
Dorset Police	4186
Durham Constabulary	6378
Dyfed Powys Police	3386
Gloucestershire Constabulary	3387
Greater Manchester Police	40857
Gwent Police	5453
Hampshire Constabulary	10979
Hertfordshire Constabulary	12825
HMRC	12731
Humberside Police	5360
Kent & Essex SCD*	18149
Lancashire Constabulary	18517

Leicestershire Police	10126
Lincolnshire Police	3994
Ministry of Defence Police	145
Merseyside Police	25356
Metropolitan Police Directorate of Professional Standards	750
Metropolitan Police Communications Intelligence Unit	103602
Metropolitan Police Counter Terrorism Command	3360
Norfolk Constabulary & Suffolk Constabulary	6654
North Wales Police	5573
North Yorkshire Police	4560
Northamptonshire Police	7872
Northumbria Police	8744
Nottinghamshire Police	13293
Police Scotland	44158
PSNI	8228
Royal Air Force Police	49
Royal Military Police	275
Royal Navy Police	62
National Crime Agency	65212
South Wales Police	10159

Lancashire County Council	24
Leicestershire County Council	12
Lincolnshire County Council	2
London Borough of Brent Council	4
London Borough of Bromley Council	21
London Borough of Camden Council	4
London Borough of Croydon Council	3
London Borough of Enfield Council	57
London Borough of Islington Council	11
London Borough of Lambeth Council	9
London Borough of Newham Council	4
London Borough of Wandsworth Council	11
Newport City Council	11
Norfolk County Council	2
North Kesteven District Council	5
North Lanarkshire Council	3
North Lincolnshire Council	12
North Yorkshire County Council	20
Northumberland County Council	3
Nottinghamshire County Council	20
Oldham Metropolitan Borough Council	1
Plymouth City Council	5
Preston City Council	2
Redcar & Cleveland Borough Council	16
Rhondda Cynon Taff County Borough Council	12
Slough Borough Council	2
South Gloucestershire Council	2
Staffordshire County Council	11
Stockton On Tees Borough Council	6
Stoke on Trent City Council	32
Suffolk County Council	6
Surrey County Council	17

Thurrock Borough Council	7
Torbay Borough Council	4
Warrington Borough Council	8
West Berkshire Council	2
West Sussex County Council	3
Worcestershire County Council	3
York City Council	25
TOTAL	**724**

The following local authorities made applications but acquired no data:

Barnsley Metropolitan Council
City of London Corporation
Cumbria County Council
East Sussex County Council
Elmbridge Borough Council
Gloucestershire County Council
London Borough of Barking & Dagenham Council
London Borough of Merton Council
Mole Valley District Council
Oxfordshire County Council
Sheffield City Council
St. Helens Metropolitan Borough Council
Tewkesbury Borough Council
Wakefield Metropolitan District Council
Warwickshire County Council
Watford Borough Council
Wiltshire Council

Annex B: Public Authorities' Communications Data inspection scores

Intelligence Agencies:

GCHQ	Good
MI5	Good
SIS	Good

Law Enforcement Agencies:

Bedfordshire Police	Good
British Transport Police	Good
Cambridgeshire Constabulary	Good
Cheshire Constabulary	Good
City of London Police	Good
Cleveland Police	Good

Merseyside Police	Good
MET CTC	Good
Met DPS	Good
Met MIB	Good
Ministry of Defence Police	Good
National Crime Agency	Good
Norfolk & Suffolk	Good
North Wales Police	Good
North Yorkshire Police	Good
Northamptonshire Police	Good
Northumbria Police	Good
Nottinghamshire Police	Good
Police Scotland	Good
PSNI	Good
RAF	Good
Royal Military Police	Good
Royal Navy Police	Good
South Wales Police	Good
Staffordshire Police	Good
Surrey Police	Good
Sussex Police	Good
Thames Valley Police	Good
UKBA	Good
West Mercia & Warwickshire	Good
West Midlands Police	Good
Wiltshire Police	Good
Avon & Somerset Constabulary	Satisfactory
Devon & Cornwall Police	Satisfactory

Lancashire Constabulary	Satisfactory
Leicestershire Police	Satisfactory
South Yorkshire Police	Satisfactory
West Yorkshire Police	Satisfactory

Other Public Authorities:

Competition & Markets Authority	Good
Department for Transport -Rail Accident Investigation Branch	Good
Department of Enterprise Trade and Investment Northern Ireland	Good
Financial Conduct Authority	Good
Health & Safety Executive	Good
HMPS NOMS	Good
IPCC	Good
MHRA	Good
NAFN	Good
NHS Protect / CFSMS	Good
Police Ombudsman for Northern Ireland	Good
Serious Fraud Office	Good
Maritime & Coastguard Agency	Satisfactory

Annex C: Prisons Inspection Scores

HMP Ashfield	Good	HMP Sudbury	Good
HMP Askham Grange	Good	HMP Thameside	Good
HMP Aylesbury	Good	HMP Thorn Cross	Good
HMP Belmarsh	Good	HMP Usk	Good
HMP Bristol	Good	HMP Wakefield	Good
HMP Bronzefield	Good	HMP Wandsworth	Good
HMP Dartmoor	Good	HMP Warren Hill	Good
HMP Durham	Good	HMP Werrington	Good
HMP East Sutton Park	Good	HMP Wetherby	Good
HMP Feltham	Good	HMP Whatton	Good
HMP Full Sutton	Good	HMP Wymott	Good
HMP Gartree	Good	HMP Cardiff	Satisfactory
HMP Hatfield	Good	HMP Coldingley	Satisfactory
HMP Haverigg	Good	HMP Doncaster	Satisfactory
HMP Hindley	Good	HMP Featherstone	Satisfactory
HMP Hollesley Bay	Good	HMP Garth	Satisfactory
HMP Huntercombe	Good	HMP Grendon	Satisfactory
HMP Isle of Wight	Good	[illegible]	[illegible]

Annex D: Serious Errors

Error Investigation 1

Error by:	Public Authority
Human or Technical:	Human
Cause:	Telephone number incorrectly recorded within a witness statement.
Data Acquired:	Subscriber information relating to a mobile telephone number.
Description:	A police force was conducting an investigation into blackmail. They made an application for subscriber information based upon the telephone number incorrectly recorded in a key witness statement. Based on the subscriber information the police visited a postal address, but no one was at home. Local enquiries suggested the occupiers were abroad. The subscriber's name and personal details were placed onto the Police National Computer (PNC) as wanted in connected with blackmail. Two months later the subscriber was arrested on his return to the UK. Following an interview in which the subscriber protested his innocence, further applications for communications data were made. These proved that the arrested person was not involved in the alleged offence.
Consequence:	An innocent person was arrested and interviewed.

Error Investigation 2

Error by:	Public Authority
Human or Technical:	Human
Cause:	Telephone number incorrectly transposed from a witness statement.
Data Acquired:	Subscriber information relating to a mobile telephone number.

Description:	A police force was conducting an investigation into a business address receiving harassing calls of a sexual nature. The witness statement correctly identified the offending number. This number was incorrectly typed into the police force's crime recording system. When the force made an application for subscriber information, the applicant used the incorrect number within the crime recording system. The police visited the subscriber's postal address. They were not at home, but the police were able to speak via telephone and arranged an interview at a local police station. Before the appointment, the subscriber obtained his own billing information. He was able to prove that he had not been in contact with the affected business number. Further applications for communications data were then made by police and a check of the witness statement provided the absolute proof that an error had been made.
Consequence:	The police visited the home of an individual unconnected with the investigation and arranged an interview.

Error Investigation 3

Error by:	Public Authority
Human or Technical:	Human
Cause:	Incorrect month and year provided to a CSP.
Data Acquired:	Subscriber information relating to an IP address.
Description:	A police force was conducting an investigation into a social media username that was using social media to incite sexual acts by children. The applicant made two accurate applications. But when transposing the data in a further application, the month and year were incorrectly typed in. Only this one of the three requests brought back a name and postal address. Following a series of circumstantial coincidences, officers executed a warrant, arrested the householder, and seized his electronic devices. During his interview these coincidences were explained, and the transposition error identified.
Consequence:	A search warrant was executed at an address unconnected with the investigation. Devices were seized for forensic examination, and an innocent person was arrested and interviewed.

Error Investigation 7

Error by:	Communications Service Provider (CSP).
Human or Technical:	Human
Cause:	Transposition error made by the CSP disclosure officer when entering a timeframe into a manual system.
Data Acquired:	Contact telephone number linked to a WiFi account.
Description:	A public authority was investigating a serious crime. To identify the offender or potential witnesses, they made a WiFi access application for users connected to a specific WiFi hub. When the CSP received the request, their system required them to manually type in the request. During this transposition, an error was made in the date/time stamp. The incorrect result led the police to a telephone whose owner was based locally. He was visited by police officers. Because he had an alibi, the police questioned their information and worked out that an error had been made.
Consequence:	The police contacted an individual unconnected with their investigation.

Error Investigation 8

Error by:	Public Authority
Human or Technical:	Human
Cause:	Failure to convert a US date format (mm.dd.yyyy).
Data Acquired:	Subscriber information relating to an IP address.
Description:	A police force sought to resolve a series of IP addresses associated with child sexual exploitation. These results were listed in the US date format. The applicant correctly converted all but two back into the UK format. As a result, subscriber checks on these two were incorrect. Based on the incorrect check, the police obtained and executed a search warrant. During the search, the officers suspected there had been an error and confirmed this by referring to the original data.
Consequence:	The police conducted a search of an address unconnected with their investigation.

Error Investigation 9

Error by:	Public Authority
Human or Technical:	Human
Cause:	Incorrect day of the month used to resolve a particular IP address.
Data Acquired:	Subscriber information relating to an IP address.
Description:	A police force was investigating child sexual exploitation by a particular username on social media. A suspect had been identified and arrested. The applicant wished to establish from where the suspect had been accessing his social media account. They carried out subscriber checks for the IP addresses where the account was first registered, when the images had been shared, and before and after his arrest. When the IP information was passed to the CSP, the wrong date was typed in. This generated an incorrect result, outside the force area, in addition to correct results for those requests which had been typed in correctly. An enquiry was made with the occupant of the incorrect address. The police who visited the address found an elderly woman who had no connection to the suspect. This caused the police to look again at their data, at which point they realised the mistake.
Consequence:	The police contacted an individual unconnected with their investigation.

Error Investigation 10

Error by:	Public Authority
Human or Technical:	Human
Cause:	Telephone number incorrectly recorded within a witness statement.
Data Acquired:	Subscriber information relating to a mobile telephone number.

Description:	A police force was conducting a fraud investigation. They made an application for subscriber information based on a telephone number incorrectly recorded in a victim's witness statement. The subscriber was invited into a police station for interview. As a result of the interview, the authority realised an error had been made.
Consequence:	An innocent person was interviewed by the police.

Error Investigation 11

Error by:	Public Authority
Human or Technical:	Human
Cause:	Telephone number incorrectly transposed.
Data Acquired:	Subscriber information relating to a mobile telephone number.
Description:	A police force was trying to locate a missing person using their mobile number, provided to police by a family member. The number was incorrectly typed into the force's records system. As a result, the application to find calls made by the missing person was based on the wrong number. Four numbers were called by this incorrect number. When the police visited the addresses associated with three of these numbers, and found no link to their investigation, they realised a mistake had been made.
Consequence:	The police visited three premises unconnected to their search then interviewed the people at these premises. This delayed the search for the missing person, who was eventually found safe and well.

Error Investigation 12

Error by:	Public Authority
Human or Technical:	Human
Cause:	Transposition error when copying an IP address from one system to another.

Data Acquired:	Subscriber information relating to an IP address.
Description:	A police force was conducting an investigation into the sexual exploitation of children. Information relating to a suspect's use of social media was transferred from one system into another. During this process, a transposition error changed one digit within an IP address. The public authority subsequently made an application for subscriber information based on the wrong IP. Based on this result, police visited the subscriber's postal address. Two men connected to this household were arrested and their devices seized for forensic examination. Following vehement denials, and the police having failed to find anything suspicious, both were released on bail. Following their release, the activity under investigation continued. A further subscriber check, this time of the correct IP address, gave a different result.
Consequence:	The police searched an address unconnected with their investigation, arrested and interviewed two innocent persons, and carried out forensic searches of their electronic devices.

Error Investigation 13

Error by:	Public Authority
Human or Technical:	Human
Cause:	Incorrect day and month typed into an IP resolution request.
Data Acquired:	Subscriber information relating to an IP address.

Description:	A police force was conducting an investigation into the use of blackmail to incite sexual acts by children over social media. The force made a series of accurate applications to identify the person using the offending account. In their final application, a request was made to find the broadband account used to first register the username. When sending this information to the CSP, a transposition error changed the day and month. The name and address received in response to this incorrect information became the base upon which an intelligence package was built. This intelligence was sent to another force who executed a search warrant at the incorrect address. Officers seized a large number of devices for forensic examination. All four occupants, including two children, were subsequently interviewed voluntarily. Because of the possible threat to the children at the address, social services were called in to assist, and briefly separated the children from their parents. The family's solicitor received the IP resolution results through the legal disclosure process. This was queried by the account holder, and the error was revealed.
Consequence:	The police searched an address unconnected with their investigation, carried out forensic examination of a large number of devices owned by innocent people and conducted voluntary interviews of four people. This included two children who were then subject to formal safeguarding processes, including being separated from their parents for a weekend.

Error Investigation 14

Error by:	Public Authority
Human or Technical:	Human
Cause:	Misinterpretation of communications data.
Data Acquired:	Subscriber information relating to an IP address.
Description:	A police force was conducting a fraud investigation. They made a series of accurate applications to identify the person behind fraud conducted through a website. The results linked an individual to the fraudster's online account and subsequent contact with the victim. Arrangements were made for this individual to attend a police station for a voluntary interview. During the interview, it became apparent that a misinterpretation of the data had occurred. Rather than identifying them as the user of the fraudulent account, they were, in fact, the person who had set up WiFi at a local event.

Consequence:	The police conducted a voluntary interview of an innocent person.

Error Investigation 15

Error by:	Public Authority
Human or Technical:	Human
Cause:	Telephone number incorrectly transposed into an application for communications data.
Data Acquired:	Call data records and consequential subscriber information.
Description:	A police force was investigating the activities of a Registered Sex Offender (RSO). In an application to a CSP, a digit of a telephone number was entered incorrectly. The result led an officer to apply for subscriber data for four telephone numbers the incorrect number had called. Three of these numbers belonged to women. A decision was taken to visit each as a preventative measure. Once all of the visits had been carried out, no connection to the RSO was established. This caused the officer to revisit their information, and identify the error.
Consequence:	The police visited the homes of and spoke to three people unconnected with their investigation.

Error Investigation 16

Error by:	Public Authority
Human or Technical:	Human
Cause:	Incorrect time conversion.
Data Acquired:	Subscriber information relating to an IP address.

Cause:	Telephone number incorrectly recorded in a police force's intelligence system.
Data Acquired:	Subscriber information and call records relating to a mobile telephone number.
Description:	A police force was investigating a murder. Officers decided to conduct analysis of numbers linked to the investigation in order to eliminate them from their lines of inquiry. They made an application to obtain the subscriber details and associated call records data for one of these numbers, which had been recorded incorrectly in a police database. The data returned placed its user and all of its activities hundreds of miles away from where the murder took place. The officer made contact with the number, and was satisfied that the person was not connected with the murder. The officer referred back to the original documentation and noticed that an error had been made. Over the next few days, the recipient of the call became worried that it might not be genuine and visited his local police station.
Consequence:	The police contacted an individual unconnected to their investigation.

Error Investigation 20

Error by:	Public Authority
Human or Technical:	Human
Cause:	Misinterpretation of communications data.
Data Acquired:	Subscriber information relating to an IP address.

Description:	A public authority had been investigating the activities of a paedophile ring. This led to a series of arrests and the seizure of devices used by the ring to share indecent images of children. The next stage of the investigation looked at the various contacts of those arrested. The activities of two such usernames were the subject of an application to identify the broadband account holders for various IP address. In the application, the force backdated the IP addresses of the usernames' most recent logons to the time and dates when images had been shared from the seized computer. This was based on a lack of understanding about how dynamic IP addresses work: that the date/time stamp is a critical part of IP address resolutions and cannot be changed. This meant that the results returned were not related to the investigation. The force used them as the basis for an intelligence package, which was sent to two other police forces. One force, on reviewing the intelligence package, noticed the error. Unfortunately, this was not in time to stop the second force from searching a property, making an arrest and conducting forensic examinations of seized electronic devices.
Consequence:	The police searched an address unconnected with their investigation, and arrested and interviewed an innocent person as well as conducted a forensic examination of an electronic device associated with that person.

Error Investigation 21

Error by:	Public Authority
Human or Technical:	Human
Cause:	Misinterpretation of communications data.
Data Acquired:	Subscriber information relating to telephone number.

Consequence:	The CSP wrote to all the relevant public authorities affected. None identified any significant impact on their operations.

Error Investigation 25

Error by:	Communications Service Provider (CSP)
Human or Technical:	Technical
Cause:	Following a system upgrade, a CSP noticed that it had been providing incorrect data to public authorities from its previous system.
Data Acquired:	Subscriber information relating to an IP address.
Description:	Following a systems upgrade, historical comparisons were conducted between the new and old data repositories. This testing found anomalies between the results provided by the older system and that of the new. The CSP investigated and found the error to be within the old and not the new system. This meant that certain sorts of requests, which had only occurred four times, risked being incorrect. The requesting authorities were immediately notified. As a result, the authorities did not take executive action.
Consequence:	The CSP contacted the relevant public authorities, who stopped any planned action.

Error Investigation 26

Error by:	Communications Service Provider (CSP)
Human or Technical:	Technical
Cause:	A technical issue brought about a backlog of files. During its repair, a series of files were eliminated.
Data Acquired:	Call Data Records relating to 21 CDRs.

Description:	A backlog developed in a CSP's call data record. Instead of bringing this data into their wider database, they inadvertently eliminated a series of files. As a result, these did not show up in any searches. Once this was discovered, the CSP investigated. They found that 21 requests were made, which should have returned results from the eliminated data. Each request was rerun and the correct results provided to the relevant public authority.
Consequence:	The CSP wrote to all of the relevant public authorities affected. None identified any significant impact on their operations.

Error Investigation 27

Error by:	Communications Service Provider (CSP)
Human or Technical:	Technical
Cause:	O2 Locations
Data Acquired:	Cell locations for SMS (Text) data.
Description:	CSP merging two services to better support communications data requests made by public authorities. When the merger was postponed, the systems were reset. This affected location data results for text messages. The issue was fixed within a week, but in that time, 1,246 SMS locations in 600 requests had the potential to be inaccurate.
Consequence:	The CSP wrote to all of the relevant public authorities affected. In 46 cases, the corrected call data record was brought into evidence replacing what had been first supplied. In 10 of these, the Crown Prosecution Service (CPS) was required to reconsider the change as new evidence. Under the Criminal Procedure & Investigations Act (CPIA), a determination was made on whether the evidence undermined the prosecution or assisted the defence.

Error Investigation 28

Error by:	Public Authority
Human or Technical:	Human
Cause:	The wilful and unauthorised acquisition and disclosure of communications data.
Data Acquired:	Incoming call data and consequential subscriber information relating to a residential landline telephone number.
Description:	A police force investigated a domestic violence abuser, who was consequently convicted at Crown Court of assaulting his estranged wife. The prosecution case was, in part, dependent upon the acquisition of communications data to evidence harassing calls received by the victim. The investigator sought to attribute calls to the defendant and, to do so, an application was submitted to identify incoming calls to what was believed to be the victim's landline home telephone. The investigator reviewed the resultant data and identified that the victim had provided the wrong number. The investigator provided the SPoC accredited officer with the correct number which they processed through the CSP portal, without the authority of a designated person. They secured 6 months of unauthorised incoming call data. The SPoC officer identified a mobile number from this data, on which he requested subscriber information. Again, this was done without the necessary authority of a designated person. The SPoC officer's actions were identified by colleagues who brought the matter to the attention of their senior manager and IOCCO. The SPoC officer is being investigated by the Professional Standards Department and further breaches, attributable to the same SPoC officer, have been raised with IOCCO.
Consequence:	The prosecution in the case of domestic abuse was, in part, dependent upon the acquisition of the unauthorised communications data. The Crown Prosecution Service and defence team were informed, by the senior responsible officer, of the unauthorised access to data. Investigations of other breaches resulting from wilful acquisitions by the same SPoC officer are ongoing.

Error Investigation 29

Error by:	Public Authority
Human or Technical:	Human
Cause:	Applicant invited CSP to use exemption under DPA to disclose CD.
Data Acquired:	Log-in history determining from where access to an 'app' had occurred.
Description:	A police force sought to determine the location or locations from where a victim had accessed three 'apps' from their electronic device (for example, their mobile phone or tablet) over several days. The investigator, acting on incorrect advice, engaged directly with the CSP who operated the 'app'. They asked them to use exemptions under the Data Protection Act 1998 to disclose communications data to provide the log-in history of that user. The CSP complied with this request. The error was discovered when the investigator later submitted a subscriber check for the IP.
Consequence:	This error highlights that police investigators are not always aware of the very broad meaning of a 'telecommunications service' within RIPA (see sections 2(1) and 81(1) and paragraph 2.16, 2.17 & footnote 4 of the Code of Practice accompanying Chapter 2 of Part 1 RIPA). To be clear: the definition is extremely broad. Any requesting of information relating to online activity may well fall under RIPA. IOCCO has shared details of the error investigation and report to help the College of Policing to identify training requirements within public authorities (see paragraphs 8.4 and 9.2 of the Code of Practice accompanying Chapter 2 of Part 1 RIPA).

CCS1217634744
978-1-5286-0174-0