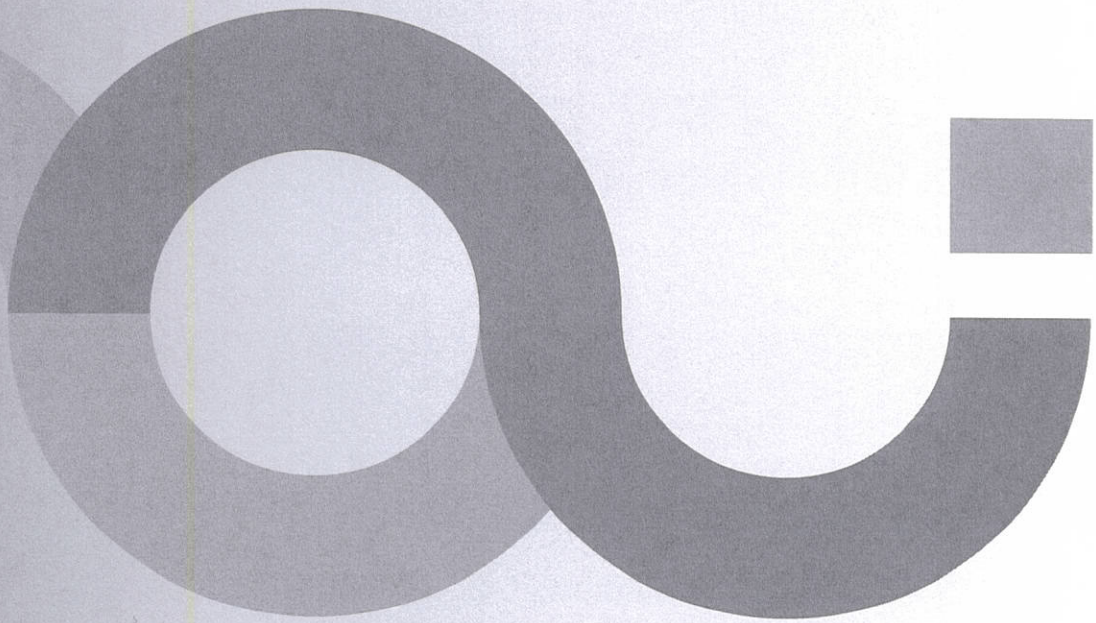
Report of the Interception of Communications Commissioner

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

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

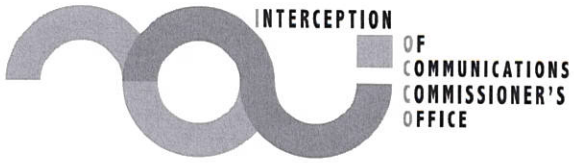
Any enquiries regarding this publication should be sent to: info@ipco.gsi.gov.uk

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



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,

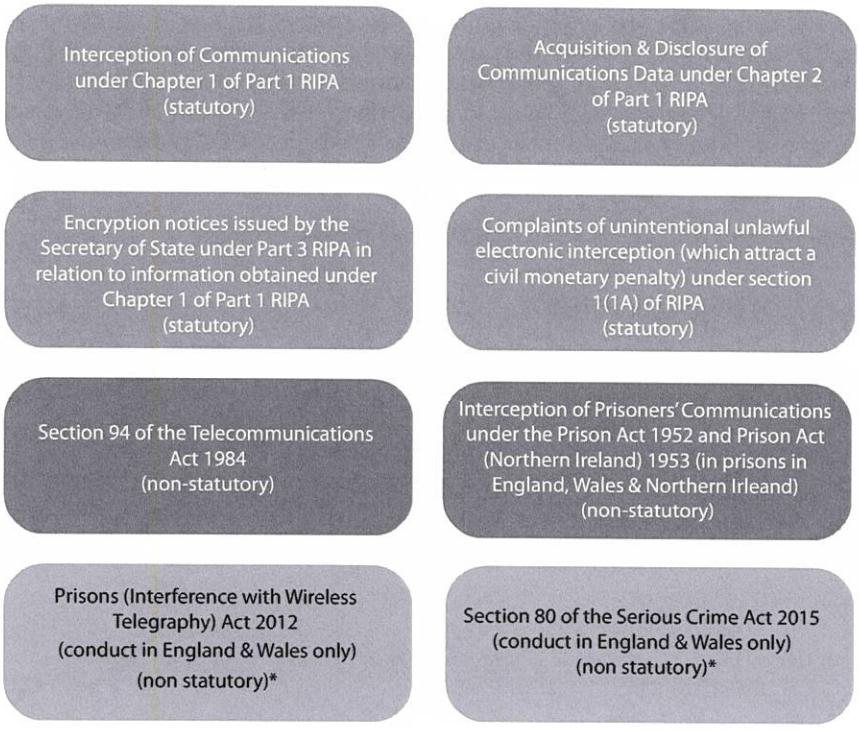
The Rt Hon. Sir Stanley Burnton
Interception of Communications Commissioner

Contents

IOCCO's Role

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.

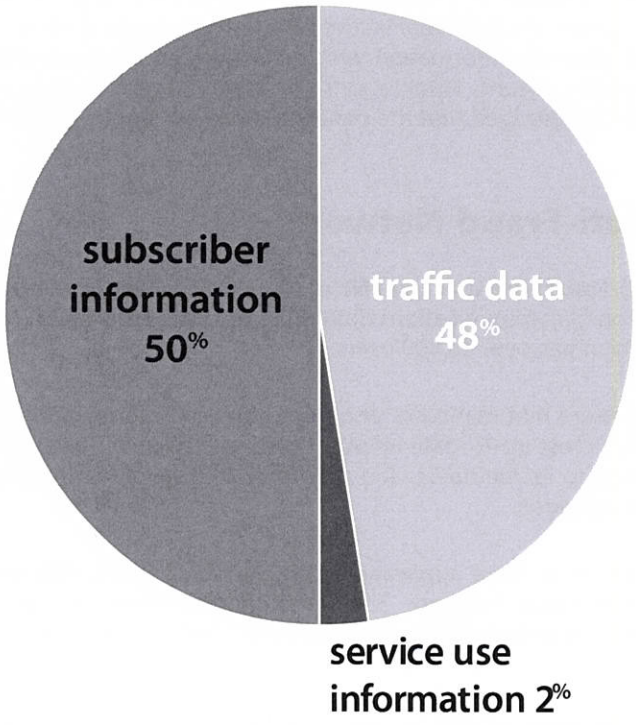
Statistics

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.

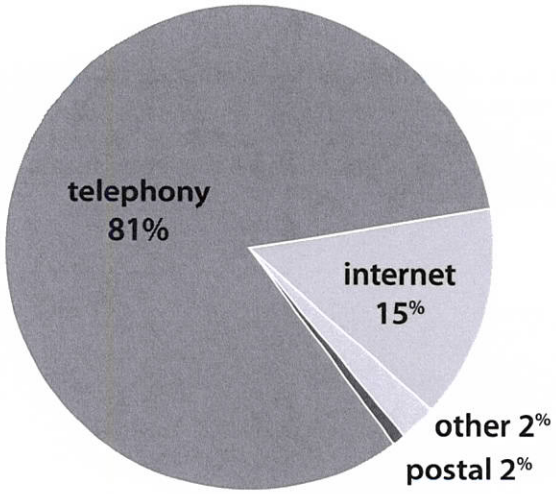
Types of data. 50% of the data acquired was subscriber information, 48% was traffic data and 2% service use information.

Figure 2 *Type of Data.*



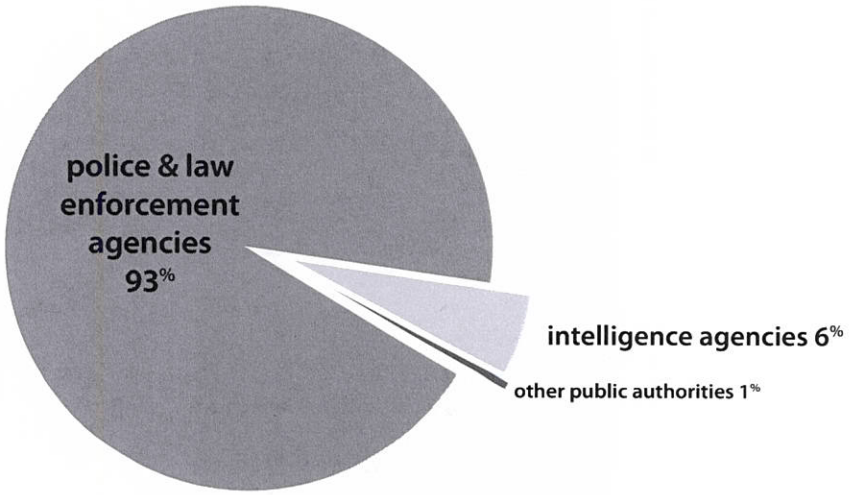
Most of the acquired items of data (81%) related to telephony, such as landlines or mobile phones. Internet identifiers, for example email or IP addresses, accounted for 15% of the acquired data. 2% of requests were related to postal identifiers.

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.*

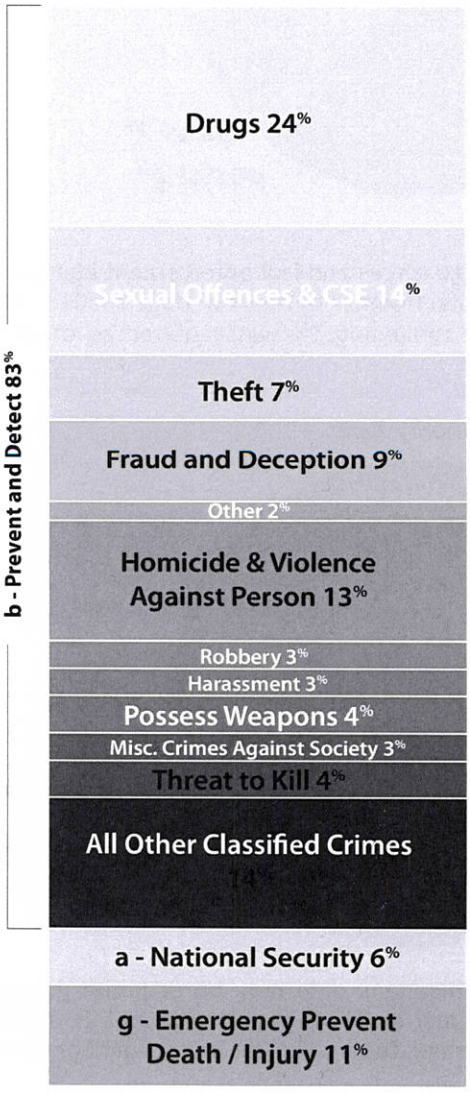


Urgent requests. Communications data may be acquired in exceptionally urgent circumstances through an oral application and approval. It might be the case, for example, that there is an immediate threat to life, or an urgent operational requirement,

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.

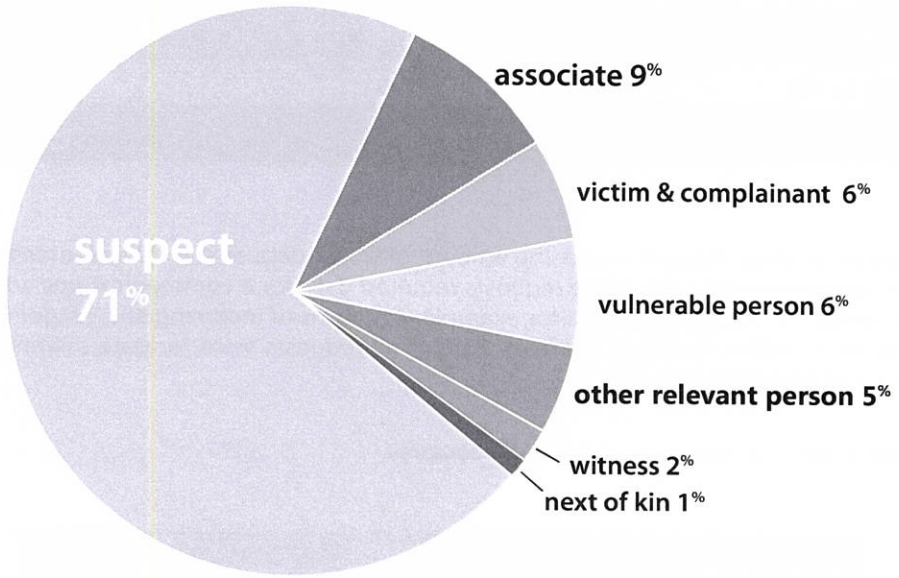
Figure 5 *Crime Type.*



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.*

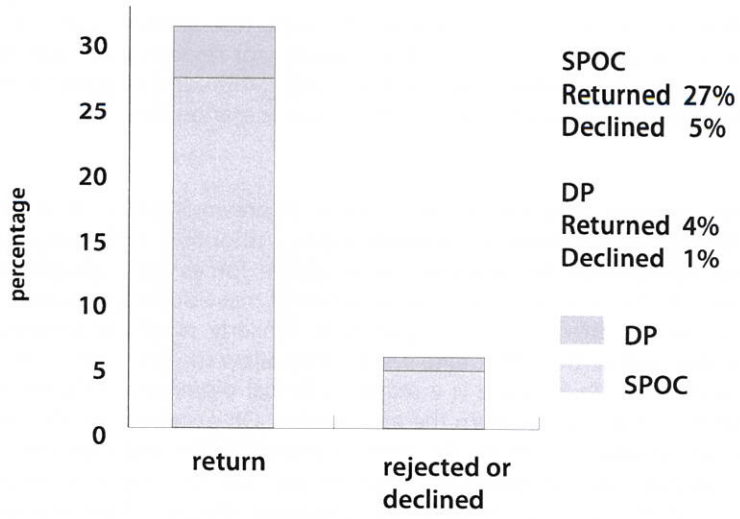
Less than a day	21%
1 to 7	9%
8 to 14	5%
15 to 30	10%
31 to 90	24%
91 to 120	7%
121 to 240	10%
241 to 365	8%
over 365	6%

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.*

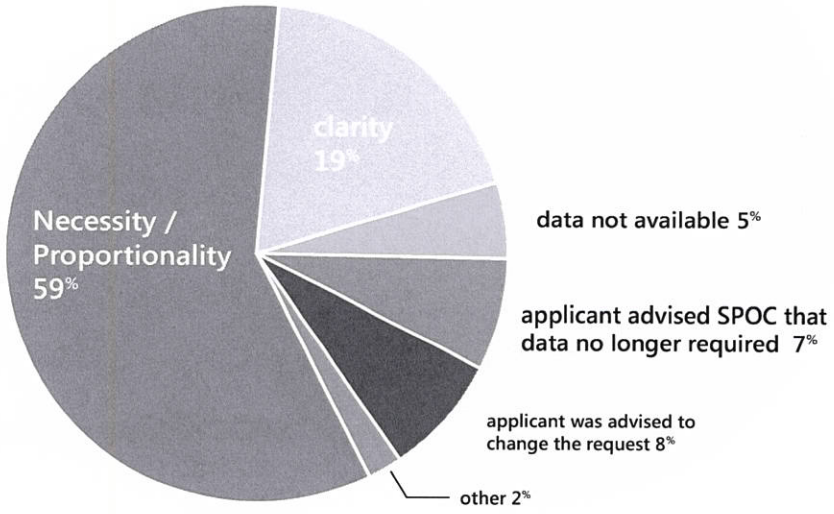
Period of data requested	Percentage
Less than 1 day	25%
1-7 days	15%
8-14 days	8%
15-30 days	13%
31-90 days	20%
91-120 days	6%
121-240 days	7%
241-365 days	3%
Over 365 days	3%

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**).

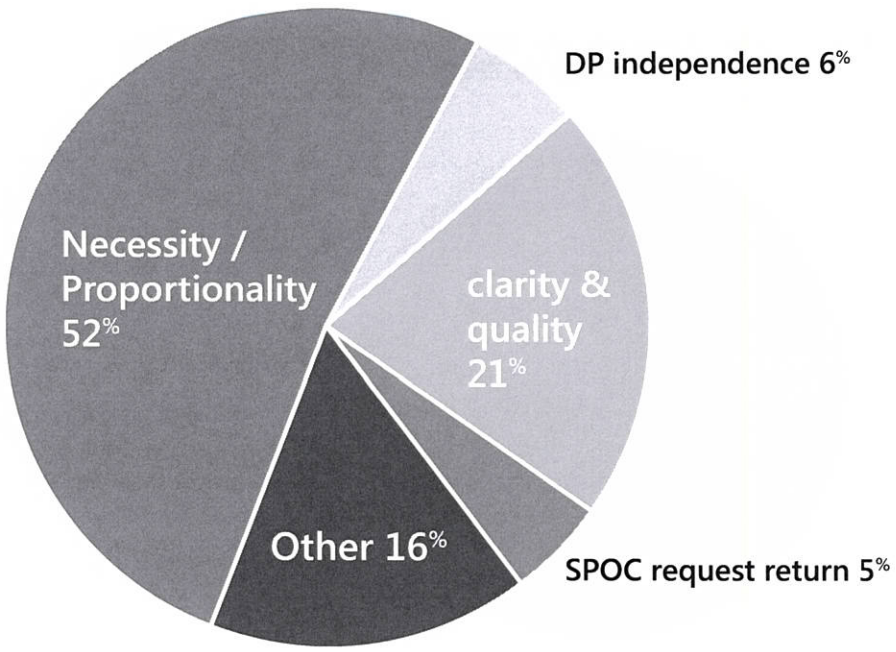
Figure 8 *breaks down the reasons why applications were returned for further development or declined by the SPoC.*



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.*

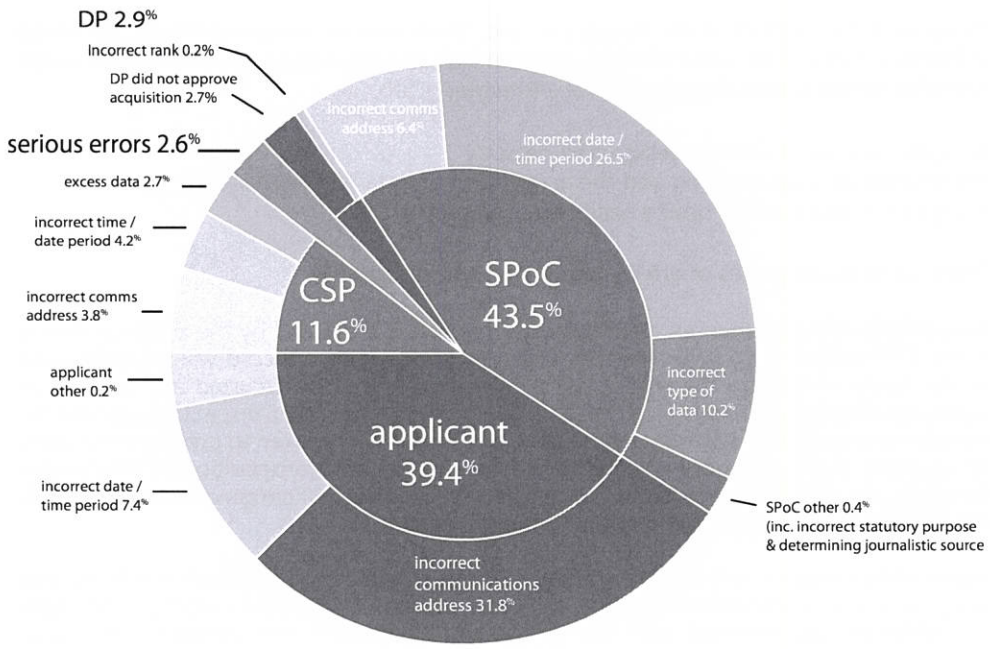


Figure 10 shows the breakdown of the 1,101 errors that occurred in 2016, by responsible party and cause. A comparison with the 2015 figures reveals that the biggest single cause of error remains the submission of incorrect communications addresses by applicants. SPoCs are responsible for 43.3% of errors. 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 mak[redacted]

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