Half-yearly report of the Interception of Communications Commissioner

July 2015

The Rt Hon.
Sir Anthony May

Half-yearly report of the Interception of Communications Commissioner

July 2015

Presented to Parliament pursuant to section 58(6) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 16th July 2015

Laid before the Scottish Parliament by the Scottish Ministers 16th July 2015

HC 308

SG/2015/105

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

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

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

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

Print ISBN 9781474123235

Web ISBN 9781474123242

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

ID 06071501 07/15

Printed on paper containing 75% recycled fibre content minimum

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

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

16th July 2015

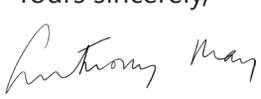
Dear Prime Minister,

I am required by section 58(4) of the Regulation of Investigatory Powers Act (as amended by section 6 of the Data Retention and Investigatory Powers Act (DRIPA)) to make a report to you with respect to the carrying out of my statutory functions as soon as practical after the end of each year and, after the end of each half year. In March 2015 you laid my first report for this year in Parliament which covered the period January-December 2014. I now enclose my half-yearly report which, as well as providing the required update on the implementation of DRIPA, also provides some timely detail about other work my office has undertaken recently.

As you know this will be my last report to you after my decision to stand down from the position of Interception of Communications Commissioner. It has been a privilege to undertake this role. During my tenure my office has performed its inspection duties, undertaken a number of high profile inquiries and contributed significantly to the various reviews of legislation and oversight that are continuing. There is much more work to be done and IOCCO remains committed to informing the public and Parliament better about our work and to ensuring there is greater transparency and accountability of public authorities' use of intrusive RIPA powers.

You are required to lay a copy of my half-yearly reports before each House of Parliament (section 58(6)) together with a statement as to whether any matter has been excluded because it has appeared to you, after consulting me, that publication of that matter would be contrary to the public interest or prejudicial to matters specified in section 58(7) of RIPA. As with my March 2015 report, there is again no suggested confidential annex or matters which I recommend should be excluded from publication. You may, of course, decide otherwise, but my expectation is that you will feel able to lay this entire report before Parliament.

Yours sincerely,



The Rt Hon. Sir Anthony May
Interception of Communications Commissioner

Contents

Section 1
Introduction

1.1 Under the requirements of section 6 of the Data Retention and Investigatory Powers Act (DRIPA), which received Royal assent on 17th July 2014, I am now required to produce half-yearly reports in addition to my annual reports. The primary purpose of these half-yearly reports was to address the concerns expressed by Parliament during the passing of the DRIP Bill that the legislation might increase or extend the powers that public authorities exercise, rather than merely clarify or replace those powers already in existence. This report will therefore seek to provide reassurance that the legislation is doing as intended[1].

1.2 However this on its own would make for a very slim report which, in my opinion, would not serve to inform the public better about our work, particularly at this time of significant public debate about public authorities use of these intrusive powers. For this reason, in my March 2015 report[2], I also committed in this report to providing more detail in relation to the serious communications data error investigations that my office undertook in 2014[3].

1.3 I made clear in my March 2015 report that it was our intention to continue to report the statistical information relating to the use of the powers and the findings from our inspections on an annual basis (in the first report of each year). This is because the statistical information takes two months to collate and analyse and it would be futile to complete that exercise twice a year and, our inspections of the larger volume users of communications data powers occur on an annual basis so reporting the findings and recommendations of these inspections half-yearly would provide an incomplete or misleading picture.

1.4 In this half-yearly report, in addition to providing an update on the implementation of DRIPA and the findings from our investigations into serious communications data errors, I have also included sections relevant to some of the new provisions set out in the revised Acquisition and Disclosure of Communications Data code of practice (published in March 2015) namely; the new statistical requirements; the strengthened arrangements for the independence of designated persons that consider communications data requests; and recent compliance issues identified concerning the acquisition of communications data to determine journalistic sources. In addition I will also provide an update on the new inspection regime that my office is in the process of introducing relating to section 94 of the Telecommunications Act 1984[4].

1.5 There continues to be significant public debate at present not only about the privacy implications of the public authorities' use of these intrusive powers, but also about the capabilities that the public authorities might require, the adequacy of the existing legislation and, the effectiveness of the current oversight mechanisms. On the same day

1 See section 5 of the annual report for 2014 at http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

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

3 See paragraph 7.109 of my March 2015 report http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

4 See Section 10 of March 2015 Report http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

as my March 2015 report was published the Intelligence and Security Committee (ISC) also published their Privacy vs. Security Inquiry report[5].

1.6 Since my March 2015 report there have been a number of further significant contributions to the debate. In May 2015 the report of the Investigatory Powers Review "A Question of Trust"[6] by David Anderson Q.C. (the Independent Reviewer of Terrorism Legislation) was published. We were very pleased to contribute to this important review. In December 2014 we published our written evidence[7] to the review which set out the effectiveness of the current statutory oversight arrangements, the safeguards to protect privacy, the case for amending or replacing legislation and the statistical and transparency requirements that should apply. We were pleased to note that the recommendations from the review addressed a number of the concerns and inadequacies that we highlighted. We were also pleased that the review recognised the significant efforts that my office has made to improve transparency and accountability in relation to the use of these intrusive powers through our reports to Parliament, our additional inquiries, investigations and publications and our various public engagements and social media presence. The Investigatory Powers Review report is very comprehensive and, as well as informing the public and political debate, it sets out an extensive series of proposals for reform.

1.7 Since the publication of "A Question of Trust" the Government has committed to bring forward a draft Investigatory Powers Bill by the Autumn which will be scrutinised in Parliament by a joint committee of both houses. There was a debate on these matters in the House of Commons on 25th June 2015 and one in the House of Lords on 8th July 2015. On 14th July 2015 the report by the Royal United Services Institute (RUSI) Independent Surveillance Review, entitled "A Democratic Licence to Operate"[8] was published. My office was pleased to attend a roundtable with the RUSI review in February 2015 and we also made available to them a number of our reports and publications. The Government has said that it will take into account the findings and recommendations from the ISC's Privacy and Security Inquiry report[9], the Investigatory Powers Review report and the report of the Independent Surveillance Review.

1.8 I hope that this half-yearly report, which will be my last as Interception of Communications Commissioner, will serve to contribute further to the debates. I would refer those readers who wish to understand the basic principles of communications data and lawful interception, and learn more about how we carry out our inspections and hold the public authorities to account, to my March 2015 report which sets out our comprehensive findings and recommendations.

5 http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

6 https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

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

8 https://www.rusi.org/downloads/assets/ISR-Report-press.pdf

9 http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

Section 2
Update on the Implementation of DRIPA

2.1 In my March 2015[10] report I attempted to answer the question as to whether DRIPA is doing what was intended. My office has again focused on the operational effect of sections 3, 4 and 5 and whether there have been any changes in practice or consequences not anticipated that we did not capture when undertaking our previous review.

DRIPA section 1. Requirements for CSPs to retain communications data

2.2 I noted in my March 2015 report and in our full responses to DRIPA[11] and the Investigatory Powers Review[12] that there does not appear to be a legal requirement for the Interception of Communications Commissioner or any other independent oversight body to review either a) the implementation of section 1 DRIPA which gives the Secretary of State the power to give a retention notice to a public telecommunications operator requiring it, the operator, to retain relevant communications data; or, b) whether DRIPA makes provision for the imposition of wider retention requirements than could be imposed under the Data Retention (EC Directive) Regulations 2009 which section 1 DRIPA sought to replace.

2.3 I was pleased to see a recommendation in the Investigatory Powers Review report[13] that the gaps in the arrangements relating to our current activities should be addressed.

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

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

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

2.5 I made comment in my March 2015 report that the policy effect of the amendments sought to make explicit that which was implicit in RIPA concerning extra-territorial reach.

2.6 In my March 2015 report I made the point that changes concerning the extra-territorial reach brought about by DRIPA did not appear to have changed or amended the operational practice of those public authorities using their powers under Part I, or the conduct undertaken by overseas CSPs.

10 See section 5 pages 13 to 18 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

11 See Para 1.2 http://iocco-uk.info/docs/IOCCO%20response%20to%20new%20reporting%20requirements.pdf

12 See Para's 3.61 and 3.62 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

13 See recommendation 92 on pages 301-302 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf

2.7 On communications data the general observations, principally those of the single points of contact (SPoCs)[14] within public authorities, conveyed to me were that whilst the overseas CSPs take receipt of notices requiring the disclosure of communications data, the CSPs continue to maintain that the notices cannot be enforced or compelled through civil sanction within the UK as the CSP is outside of UK jurisdiction. It is common for the CSPs to require information in addition to the notice to determine whether they are able to disclose communications data taking into account the laws within the jurisdiction in which they generate and retain the data. In the CSPs view they are disclosing the data "voluntarily" and are not required to disclose it.

2.8 Turning to interception warrants, in my March 2015 report, I made the point that some overseas CSPs are still providing voluntary assistance in very limited circumstances. The Government has still not yet enforced the duty under section 11 RIPA (as amended by DRIPA) to comply with an interception warrant.

2.9 I have concluded that the position has not changed significantly to the observations in paragraphs 2.6 and 2.7 of my March 2015 report but, a few matters are worthy of comment.

2.10 First, the Investigatory Powers Review report "A Question of Trust" was published in June 2014[15]. Chapter 11 of that report summarises the submissions made to David Anderson Q.C. by CSPs, both domestic and international and provides a helpful synopsis of what is a complex set of issues.

2.11 Second, a summary of the work of Sir Nigel Sheinwald, the Prime Minister's special envoy on intelligence and law enforcement data sharing has recently been published[16].

2.12 Third, it is worth pointing out that the Investigatory Powers Review report notes that "*there have been recent and limited signs of improving cooperation",* and the summary of the work of the Prime Minister's special envoy notes that there has been *"progress in improving short term co-operation"*. I agree with these comments and my office has seen during our inspections an increase in cooperation for urgent requests relating to counter-terrorism and other threat to life and child protection cases.

2.13 Fourth, I concur with Sir Nigel Sheinwald's comment that cooperation remains incomplete and that there is broad agreement from the CSPs and Governments concerned that there is a need to work on longer term solutions. Sir Nigel Sheinwald makes four recommendations in this regard: improve Government-to-Government cooperation; reform US / UK Mutual Legal Assistance Treaty (MLAT); build a new international framework; improve transparency and better coordinate relationships with the CSPs.

2.14 Fifth, it is clear from my office's engagement with overseas CSPs that they have a desire to operate under a clear legal mandate and this has been articulated to both

14 See paragraphs 3.22 – 3.30 of the Acquisition and Disclosure of Communications Data Code of Practice as to their roles and responsibilities

15 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf

16 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf

UK and US governments. A number of CSPs have proposed their own international framework and are advocating its adoption[17].

2.15 Finally in our reports we repeatedly highlight the important role of the Single Point of Contact (SPoC) within the public authorities in the communications data acquisition process. The Secretaries of States' warrant granting departments[18] perform a similar SPoC function with regard to interception warrants. The Investigatory Powers Review (see page 205 – paragraph 11.14) received very positive feedback on the role of the SPoC from engagement with CSPs based both within and outside of the UK:

> *A rather specific, yet important, area of complete unanimity worth highlighting was support for the SPoC arrangement (7.39 above), which was said to act both as a "quality filter" and as reassurance that there had been "a lot of checks and balances". All companies wanted it to be retained and developed. US companies described it to me as "a model for everyone" and compared it favourably to the US system, in which they could be contacted by any of "10,000 FBI agents, who don't necessarily know what they are asking for".*

DRIPA section 5. The definition of Telecommunications Service

2.16 In my March 2015 report I made the point that one of the consequences of the change to the definition was that it clarified the telecommunication services that are covered by Part I of RIPA so that it is more difficult for companies who provide internet-based services, such as webmail, to argue that they are not caught by RIPA.

2.17 I can again confirm that the change to the definition does not appear in practice to have resulted in an extension of powers.

17 https://www.reformgovernmentsurveillance.com/

18 See Para 6.8 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

Section 3
Aquisition and Disclosure of Communications Data Code of Practice

3.1 Section 71 of RIPA enables the Secretary of State to publish codes of practice relating to the exercise and performance of the powers and duties (for example within Chapter 2 of Part 1 of RIPA). After laying the draft code within both Houses of Parliament the Secretary of State may, by an order, bring that code into force.

3.2 In December 2014 the Home Office published a revised code of practice for the acquisition and disclosure of communications data for public consultation. The code was amended using the processes set out in section 71 of RIPA and came into force by Secretary of State's order on the 25th March 2015.

3.3 During our inspections in late 2014 we were very concerned that SPoCs within public authorities, especially law enforcement, seemed to be unaware of the detail of the consultation and the resultant code that was published to take account of changes in law and practice. This became very apparent as we were discussing key changes that public authorities would need to introduce, in anticipation of the revised code coming into force, and making recommendations based on the expected changes.

3.4 The period allowed by the Government for the drafting, consultation and implementation of the code was ambitious, and with hindsight, more extensive consultation with key stakeholders and more time for all to consider the issues properly would have enabled some of the provisions to be better refined to make certain matters clearer. It would also have ensured that all public authorities were aware fully of the changes and had time to consider the operational implications. As a consequence we have had to publish additional guidance to clarify elements of the code, our inspectors are finding that they are having to address knowledge gaps during inspections and, a number of public authorities are still working on implementing some of the required changes to their procedures.

New statistical requirements

3.5 For a long time we have warned of the inadequacies and flaws relating to the previous statistical requirements in the code. The previous statistical requirements lacked clarity and the counting conventions applied by the public authorities differed. This is why we have made clear in successive reports to the Prime Minister[19] that the statistics were only indicative of the amount of communications data acquired by public authorities and must be treated with caution. We also made clear that the statistics ought not to be used inappropriately to produce league table comparisons.

3.6 In 2012 we set out to the Home Office the revisions and enhancements of the statistical requirements that we believed were necessary both to assist us with our oversight role and to better inform the public about the use which public authorities make of communications data powers. We were very pleased to note that the revised

19 See pages 22-24 of our 2013 report http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf and page 47 of our March 2015 report (covering 2014) http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

code enhanced significantly the statistical requirements[20]. For example, public authorities are now required to record the crime type in cases where the data has been acquired under section 21(4)(b), the number of refusals and the reasons for those refusals, the age of the data at the time of its acquisition etc. These new requirements will improve transparency and provide for more meaningful analysis about how the powers are being used. My office is working on additional guidance concerning the revised statistical requirements. The benefits of the new statistical requirements may not be realised fully until the significant changes to public authorities systems and processes have been embedded.

Requirement for designated persons to be independent

3.7 One of the changes in the code relates to the role of the designated person (DP). Paragraph 3.12 of the code outlines that DPs **must** be independent from operations and investigations when granting authorisations or giving notices related to those operations. This is a strengthening of the previous code which stated that DPs **should not** be responsible for granting authorisations or giving notices in relation to investigations in which they are directly involved.

3.8 This policy change was brought about in response to the European Court of Justice (ECJ) Judgement which struck down the Data Retention Directive (2006/24/EC) as the directive did not include sufficient safeguards as to why and by whom such data may be accessed. The Judgment did not prevent Member States implementing their own laws requiring the retention of communications data but it did critically note that the Directive itself contained no safeguards to access to the retained data, including in relation to the independence of the person authorising access to the retained data. Within the UK, the Data Retention & Investigatory Powers Act (DRIPA) 2014 implements data retention and also requires that any access to such data is undertaken by the use of Chapter 2 of Part 1 RIPA or a court order.

3.9 My office received a number of questions from public authorities regarding this policy change and its operational consequences and on 1st June 2015 we published a circular to Senior Responsible Officers (SROs)[21] to provide clarification about the new provisions and assist public authorities to implement procedures which ensure that any acquisition of communications data is authorised by DPs who are independent of the operation or investigation.

20 See paragraphs 6.5 to 6.8 of the March 2015 code https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

21 See page 33-34 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

Applications for communications data to determine the source of journalistic information

3.10 In October 2014 due to the serious nature of the concerns reported in the media about the protection of journalistic sources and allegations that the police had misused their powers under Chapter 2 of Part I of RIPA to acquire communications data, the Rt Hon. Sir Paul Kennedy, who was at the time acting as interim Commissioner, considered it necessary to launch an inquiry and make an additional report to the Prime Minster.

3.11 In February 2015 I published the report entitled *"IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources",* setting out my office's findings into these matters. The report set out the extent to which the powers were used by police forces to identify journalistic sources, examined the appropriateness of this use, and made recommendations to ensure adequate safeguards were in place to protect journalistic sources. I was pleased that the Prime Minister accepted my recommendations straight away and committed to implement them as soon as possible. The Serious Crime Act which received Royal Assent on 3rd March 2015 amended section 71 of RIPA 2000 to require the revised code to include provision designed to protect the public interest in the confidentiality of journalistic sources.

3.12 During the debates on 16th March 2015 considering the draft revised code, the Home Office Minster for Security and Immigration (James Brokenshire) said[22]:

> *Let me turn to one of the most important new safeguards in the acquisition code: that of access to journalistic material. As the right hon. and hon. Members will know, the Interception of Communications Commissioner recently conducted an inquiry into police acquisition of journalists' communications data. The measures in the revised code are intended to give effect to his recommendations, which were accepted straight away by the Government.*
>
> *The acquisition code that we are debating stipulates that, in seeking to acquire communications data to identify or determine the source of journalistic information, law enforcement must use production orders under the Police and Criminal Evidence Act 1984 or its equivalents in Scotland and Northern Ireland. We are doing this because production orders require judicial approval. This will help to protect the freedoms that journalists enjoy in the UK.*
>
> *Whenever law enforcement is seeking the communications data of a journalist to determine sources - this includes when police are seeking to confirm or corroborate other evidence of the identity of a journalist's source - the decision on the application will be made by a judge under PACE. However, that is only a stop-gap until we can make the change through primary legislation in the next Parliament. We have therefore also published a draft clause that sets out how we would seek to enshrine the commissioner's first recommendation in primary legislation.*

22 See http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm150316/debtext/150316-0001.htm#1503165000098

3.13 The code enacted in March 2015 states at paragraphs 3.78 and 3.79:

> *In the specific case of an application for communications data, which is made in order to **identify** a journalist's source, and until such time as there is specific legislation to provide judicial authorisation for such applications, those law enforcement agencies, including the police, National Crime Agency and Her Majesty's Revenue and Customs, in England and Wales with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data. Relevant law enforcement agencies in Northern Ireland must apply for a production order under the PACE (Northern Ireland Order) 1989. Law enforcement agencies in Scotland must use the appropriate legislation or common law powers to ensure judicial authorisation for communications data applications to **determine** journalistic sources.*
>
> *Communications data that may be considered to determine journalistic sources includes data relating to:*
>
> - *journalists' communications addresses;*
> - *the communications addresses of those persons suspected to be a source; and*
> - *the communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.*

3.14 The use of the text "*....which is made in order to **identify** a journalist's source*" could have been clearer. It appears to indicate that if the source is already known to the police the restriction on the use of RIPA does not apply whereas the text "*...must use the appropriate legislation or common law powers to ensure judicial authorisation for communications data applications to **determine** journalistic sources*" appears to indicate that judicial approval must be sought even if the source is known.

3.15 What is not in doubt in my opinion is the policy intention that in circumstances where public authorities are seeking to determine journalistic sources judicial authorisation must be obtained and this will, according to the Minister, include when police are seeking to confirm or corroborate other evidence of the identity of a journalist's source.

3.16 Although I welcome the fact that the Government took steps promptly to change the legislation to include provision designed to protect the public interest in the confidentiality of journalistic sources, I commented in my March 2015 report that my recommendations required careful consideration and that the interim measures which that were introduced were not ideal. Again the lack of stakeholder engagement due to the speed at which the new legislation was implemented has resulted in a lack of clarity about the provisions. For example, it is not clear what authorisation route would be taken by public authorities who do not have powers under the Police and Criminal Evidence Act 1984 (PACE). I have commented previously that my office is concerned that a number of public authorities seem to be unaware of the changes in law and practice. I have also been very disappointed to learn that a number of Senior Responsible Officers (SROs) and SPoCs have admitted during inspections to having not read our journalist inquiry report.

3.17 Of most concern, but perhaps not of surprise bearing in mind the previous points, is that my inspectors have identified that since 25th March 2015, when the revised code came into force, two police forces have acquired communications data to identify the interactions between journalists and their sources in two investigations **without obtaining judicial approval**. These breaches were identified during our inspections. In these cases the normal RIPA process was used and the data was approved by a designated person.

3.18 In the first case a police force acquired the communications data for a journalist and a known associate who was also their source. The crime under investigation related to attempting to pervert the course of justice in the midst of an ongoing criminal trial. The trial judge was aware of the police force initiating a criminal investigation into the activities of the journalist.

3.19 In the second case a police force acquired communications data relating to a suspected journalistic source working within the police force and a former employee of the force suspected to be acting as an intermediary. No data was acquired relating to the journalists who published subsequently an article which allegedly relied on leaked information from the police employee. Criminal offences under the Data Protection Act and Computer Misuse Act relating to the passing of information acquired and retained by the police in a crime investigation were under investigation.

3.20 These cases were only very recently identified by my inspectors and I am waiting for the full details to enable me to establish whether any individual has been adversely affected by any wilful or reckless failure by any person within a public authority. If I establish that fact I will, in line with paragraph 8.3 of the code, inform the affected individuals of the existence of the Investigatory Powers Tribunal (IPT) and its role to enable them to engage the IPT effectively. In both of these cases my office has also required that the police forces inform the prosecutor of the fact that communications data has been acquired in contravention of the processes prescribed by Parliament and, of the need to review their obligations under the laws governing the disclosure of materials to the defendant or their counsel if proceedings ensue.

3.21 The actions in these cases are serious contraventions of the code, which in turn reflected the will of Parliament, in seeking to protect Article 10 of the European Convention on Human Rights ("the Convention") particularly the protection of journalists, their sources and persons who may act as intermediaries.

3.22 I think it worth revisiting an observation we highlighted our journalist inquiry report[23] regarding the zero tolerance culture that seemed to be operating within police forces:

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

> *"We also considered publications by the Independent Police Complaints Commission (IPCC), Her Majesty's Inspectorate of Constabulary (HMIC), the Association of Chief Police Officers (ACPO), the College of Policing and Elizabeth Filkin concerning the investigation of police corruption, misconduct in public office and leaks to the press. A summary of these publications is contained in Annex E (pages 49 to 55). The publications considering 'leaks to the press' and 'undeclared relationships with the press' put emphasis that a low threshold will apply to the point that a state of zero tolerance appears, in practice, to be operating. Little reference, if any, is made to Article 10 of the Convention or the published guidance from the CPS. Consequently, the publications by the IPCC, ACPO, College of Policing, HMIC and Filkin must not be considered in isolation by chief officers especially if the police are seeking to embark on investigations to identify who within an organisation has leaked information to the media."*

3.23 I ask chief officers to reflect again on Article 10 of the Convention prior to embarking on investigations to identify who within an organisation may have leaked information to the media. Police forces must ensure they comply fully with the revisions in the code whenever they are seeking communications data to determine journalistic sources, this includes when public authorities are seeking to confirm or corroborate other evidence of the identity of a journalistic source. Such applications must have judicial approval.

3.24 It is also worth reflecting on some of the positive work in this area that my inspectors have identified during recent inspections. My office has found evidence of Senior Responsible Officers (SROs) and Single Points of Contact (SPoCs) rejecting applications that have been submitted under RIPA to acquire communications data to determine journalistic sources since the new provision was enacted. In some cases investigative teams have pushed back and put the SPoCs under considerable pressure to process such requests. These cases generally relate to circumstances where the source was already known to the police and therefore the investigative teams felt strongly that the judicial provisions in the code did not apply. I have already outlined the unfortunate lack of clarity on this point and the fact that in my opinion the policy intention is that the provision includes communications data applications which seek to determine journalistic sources where the source is already known to the police and they are seeking to confirm or corroborate that fact.

3.25 In May 2015 I also noted the media articles reporting that the Metropolitan Police Service (MPS), represented by Jeremy Johnson Q.C., appeared before Mr. Justice Sweeney at the Central Criminal Court to seek communications data to determine journalistic sources in relation to Operation Elveden. The applications under PACE were heard in open court. Mr. Justice Sweeney approved all the applications, although two were granted on more limited terms than those sought by the MPS, and in doing so he said: "*normally applications would be held in private but given they are the first of their type and following the interception commissioner's report on the change of approach to applications of this type.... it seemed to me exceptional and subject to submissions it would be appropriate for them to be held in open court.*"

3.26 In summary, although the revised code includes a number of enhanced safeguards to protect privacy and provisions to improve transparency, regrettably the lack of extensive stakeholder engagement, the speed at which the legislative changes have been enacted and the resultant unrefined elements of the code mean that our inspectors appear to be fine-tuning Government policy and implementing it rather than auditing it. I would urge the Government to ensure that extensive stakeholder engagement takes place when moving forward with new legislation.

Section 4
Telecommunications Act 1984 (section 94)

4.1 In my March 2015 report[24] I set out that the Prime Minister had recently asked me to oversee directions issued under section 94 of the Telecommunications Act 1984. This oversight is on a non-statutory basis at present and I expressed my hope that this would be put on a statutory footing in the next Parliament.

4.2 Section 94 of the Telecommunications Act 1984 covers '*directions in the interests of national security etc*' and applies to the Office of Communications (OFCOM) and to providers of public electronic communications networks. It provides that the Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom. If it appears to the Secretary of State to be necessary to do so he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction. The Secretary of State shall not give a direction unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.

4.3 I made clear that I would require additional staff (and possibly technical facilities) to be able to carry out this oversight properly. Under section 57(7) of RIPA the Secretary of State must provide me with such staff as are sufficient to secure that I am able to carry out my functions properly. The Home Secretary agreed that my office could recruit additional staff for this function and my office is in the process of recruiting an inspector. Providing there are no delays in this recruitment my office anticipates that it will be able to start the formal audit regime in the last quarter of 2015. Whether my office will require further resource (staffing or technical) remains to be seen.

4.4 Since the publication of my report in March 2015 my office has also undertaken to determine the nature and full extent of the work being carried out under any directions in order to scope the oversight requirements. My office has already had some very helpful discussions with persons from a number of the public electronic communications networks that have been served with directions. There are, however, some considerable challenges in this regard. The challenges stem from the fact that the directions are secret as allowed for by statute[25], can be given by *any* Secretary of State and do not automatically expire after a certain period. There does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State. My office is therefore not yet in a position to be able to say confidently that we have been notified of all directions.

24 See Section 10 page 78 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

25 Section 94(4) of the Telecommunications Act states that the Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person. Section 94(5) states that a person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

4.5 I would recommend that provision is made in any future legislation that might encompass such directions to inform the Interception of Communications Commissioner (or any such successor oversight body) of all extant section 94 directions to enable this area to be overseen properly.

4.6 The Prime Minister's decision earlier this year to ask me to formally oversee directions issued under section 94 of the Telecommunications Act 1984 is however a good first step towards greater transparency and comprehensive oversight of any directions. The oversight, albeit on a non-statutory basis, will be extensive as it will cover:

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

4.7 My office previously provided *limited* non-statutory oversight of the use made of one particular set of section 94 directions. This oversight was limited because it was only concerned with parts of c) above. My office was, and still is, prohibited from saying any more about this oversight as the Secretary of State is of the opinion that disclosure would be against the interests set out in section 94(5) of the Telecommunications Act.

4.8 My successor will hopefully be able to provide some further information in the next report about the progress of this oversight regime. I would echo the sentiments of others[26] with regard to the avowal of any capabilities and the consolidation of relevant legislation to enable such matters to be debated and considered properly.

26 David Anderson Q.C. recommendation 9 page 286 "A Question of Trust" https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf and the Intelligence Security Committee's recommendation BBB p109 Privacy and Security Inquiry Report http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

Section 5
Communications Data Serious Error Investigations

5.1 This section of the report provides details about my office's investigations into the serious communications data errors that were reported to us in 2014[27]. Before setting out the nature of the errors and recommendations that my office made in this area I thought it would be helpful to provide some background information about the error procedures.

What is a communications data error?

5.2 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).

5.3 An error occurs 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.

5.4 **Recordable errors:** In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences. The record will explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. During our inspections we examine the recordable errors along with any steps the public authority has taken to prevent recurrence. For example, where human error such as incorrect transposition of information occurs but does not result in the wrongful acquisition or disclosure of communications data.

5.5 **Reportable errors:** In cases where an error has occurred that has led to communications data being acquired or disclosed wrongly a reportable error will arise. In some instances wrongful disclosures infringe the rights of individuals not connected with the particular investigation or operation. Reportable errors must be reported to my office in no more than five working days of 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 what steps have been, or will be, taken to ensure that a similar error does not recur. For example, where the wrong type of data or data in relation to the wrong telephone number is acquired or disclosed.

5.6 The vast majority of reportable errors are self reported to my office by public authorities and CSPs. There is a very strong culture of self reporting when things go wrong by both public authorities and CSPs. I continue to be impressed with the co-operation and dedication of staff within public authorities and CSPs both in the reporting of errors and the introduction of measures to prevent recurrence.

27 See paragraph 7.109 of the annual report for 2014 at http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

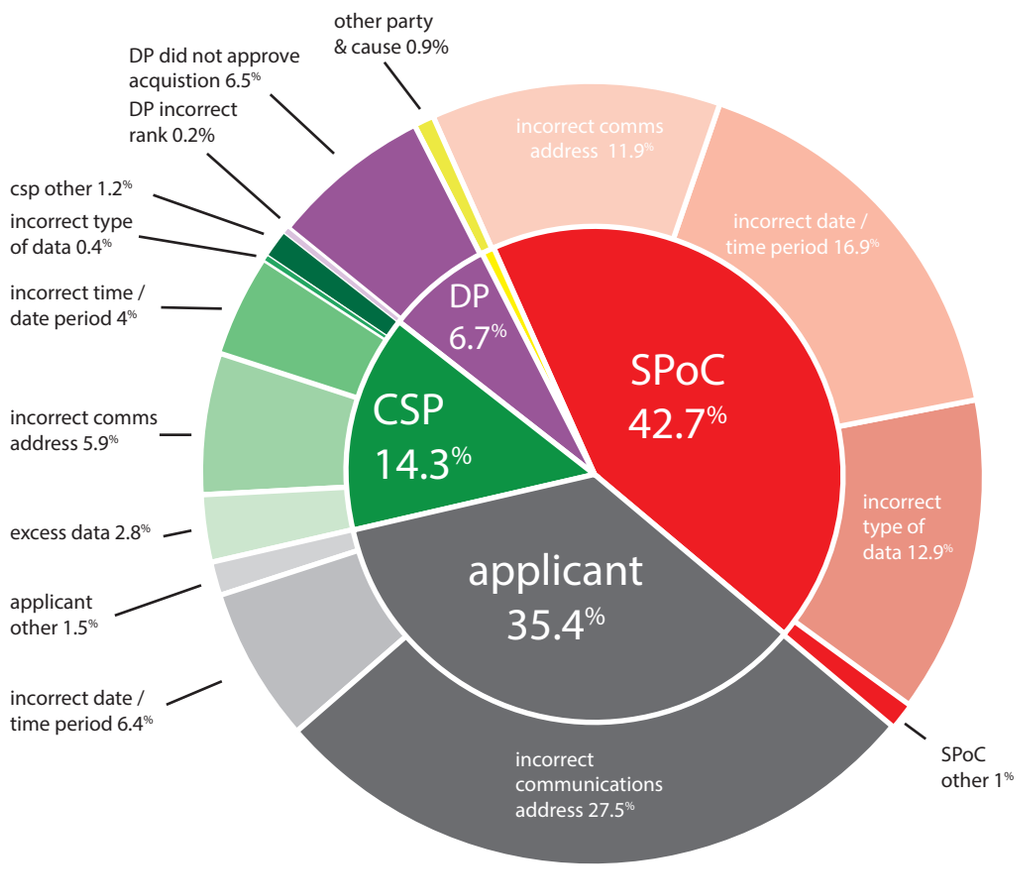
Statistics

5.7 As published in my March 2015 report, the total number of communications data errors reported to my office in 2014 was 998. 84.8% of these errors were attributable to public authorities, 14.3% to CSPs and 0.9% to other parties. Figure 1 shows the breakdown of these errors by responsible party and cause (and is a repeat of Figure 13 from my March 2015 report).

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

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

Figure 1 *2014 Breakdown of Errors by Cause*



Serious error investigations

5.10 My office would classify an error as *serious* if on initial assessment it falls into one of the below three categories:

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

2 Errors where the public authority has, as a consequence of the data, initiated a course of action that impacts on persons not connected with the investigation or operation (for example, the sharing of information with another public authority stating a person is suspected of a crime, an individual being visited or the execution of a search warrant at premises unconnected with the investigation, the arrest of a person).

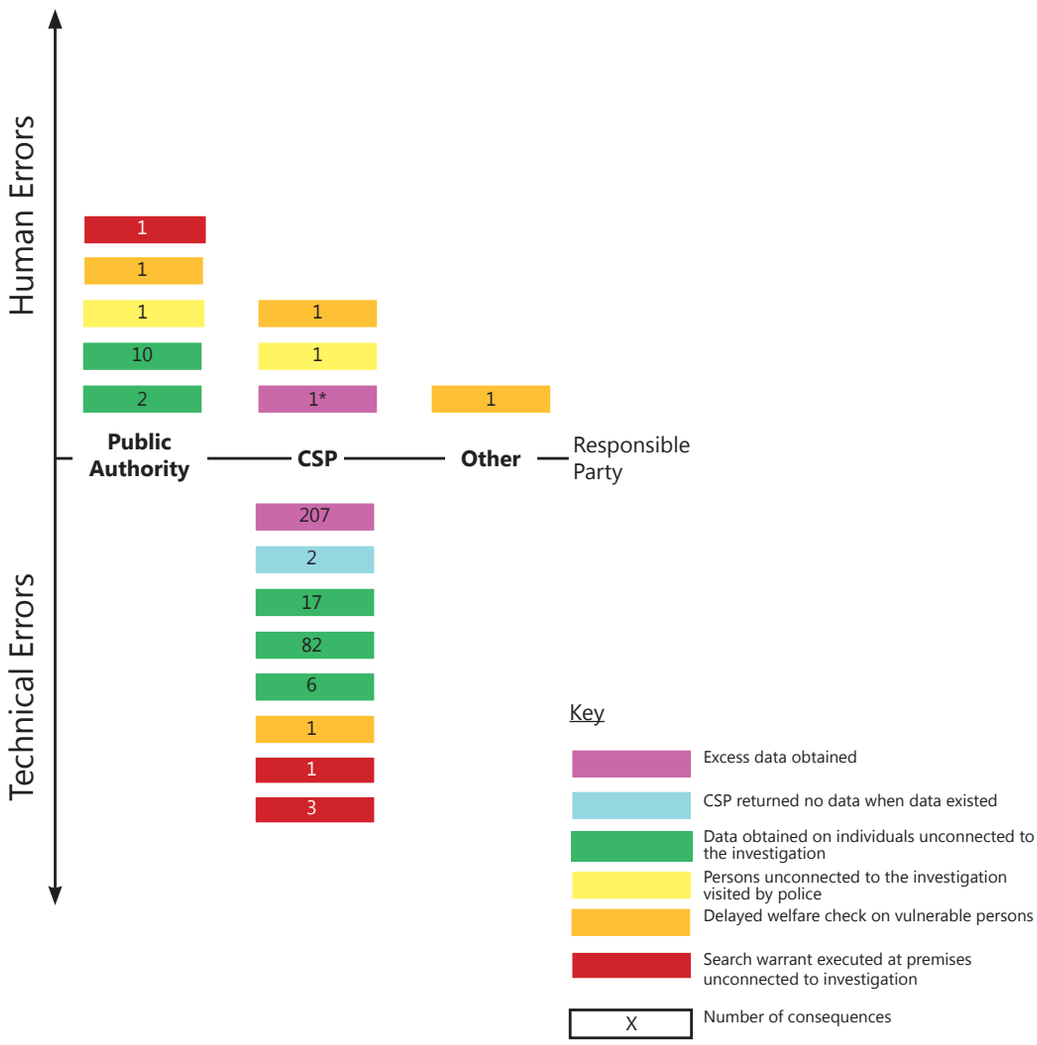
3 Errors which result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

5.11 In circumstances where a *serious* error is assessed to have occurred an inspector will be allocated to investigate fully the cause of the error, the impact of the interference on the affected individuals' rights (if applicable) and, the measures put in place to prevent recurrence. These serious error investigations are extensive and in some cases take several months to complete. In each instance early engagement takes place between the inspector and the public authorities and / or CSPs to ensure that all relevant parties are notified about the error. Immediate measures are put in place to prevent further errors and their implementation is overseen. I will provide more information on this point when discussing some of the technical CSP system errors later in this section. The consequences and impact of each error instance are then investigated in detail. My office will also ensure that any data that is wrongly acquired is deleted in line with paragraph 6.24 the code or that any excess data is managed appropriately (see paragraphs 6.26 to 6.28 of the code). Once the investigation has been concluded I will receive a detailed report setting out a summary of the incident; a full background of the circumstances leading to the error, the cause of the error and its impact; the measures put in place to prevent recurrence; and any recommendations where applicable.

5.12 In my March 2015 report I set out that 24 such error investigations had been instigated by my office in 2014. My office concluded that in 7 of the 24 cases the errors did not in the end meet the serious error criteria and therefore those cases do not form part of this report.

5.13 Figure 2 provides a breakdown of the 17 serious errors by responsible party and consequence.

Figure 2 *Serious Errors by responsible party and consequence*



Caveat: The chart shows the most serious impact to have occurred from the error. There may be other lesser impacts. For example where an error led to warrants being executed at premises unconnected to an investigation, data may also have been obtained on other individuals also unconnected to the case. Please see Annex A for full details.

* Please see Error 9 in Annex A for full details regarding the scale of the impact in this case.

Naming of the public authorities, CSPs and other parties involved in the investigations

5.14 After significant careful consideration and weighing up the strengths of the arguments for and against naming the public authorities, CSPs and other parties involved in these serious error investigations I have taken the decision not to name those involved. I have however set out whether each error was caused by a public authority, CSP or other party. There are a number of compelling reasons as to why I have taken this decision.

5.15 I started by considering the rights of those individuals who have had their privacy infringed. In some of the cases the impact on the affected individual's life was significant. I wanted to ensure that their privacy is respected and not further infringed. In all cases where there has been a very serious consequence (for example, where a search warrant has been executed at a premises unconnected with the investigation) the affected individuals are aware that the particular error occurred. It is fair to say that in the majority of cases the individuals were incredibly understanding about the cause of the error that led to their privacy being infringed. Some wanted, understandably, to put the matter behind them. Others are seeking legal redress and another consideration is that naming could prejudice ongoing or settled litigation.

5.16 I also considered the potential consequences of naming the other parties involved in these errors. Some are organisations which exist to prevent the abduction and sexual exploitation of children or, to provide support and advice to children in crisis. These organisations provide a vital service and some are staffed mainly by volunteers. I did not want the naming of those organisations to have the unintended consequence of causing a lack of trust and confidence in the abilities of such services, resulting in children failing to seek help or deterring volunteers. With regard to overseas organisations I also did not want to jeopardise existing relationships with law enforcement, especially in cases where the errors may involve CSPs who currently consider that they disclose data on a voluntary basis (see section 2 of this report).

5.17 I also had serious concerns that naming may have the unintended consequence of undermining the open and co-operative self reporting of errors. There is a real danger that the publication of the names could reduce accountability because the reporting process depends on individuals reporting at the earliest opportunity when they or their colleagues have made mistakes or when technical systems have failed. Publication of organisations' names may be construed as "naming and shaming" which, when considering human nature, may deter some from reporting errors in future and lead to a subversive error culture. This could reduce the shared desire by all parties to work together to resolve errors, prevent recurrence of errors and to strive for continuous improvement. It could perversely result in a greater impact upon an individual, or impact on a larger number of individuals, than might otherwise have been the case.

5.18 The naming of those involved would also raise a fairness issue as these 17 error investigations are not set in context against the scale or amount of data these public authorities or CSPs acquire or disclose. There were an additional 981 errors reported to my office in 2014. Naming those involved in only the 17 serious error investigations could

unfairly mislead the public about the competence of a particular public authority or CSP. For example a particular public authority or CSP might acquire or disclose considerably higher volumes of data to public authorities so without the context in relation to the error ratio the reporting would be misleading; other public authorities and CSPs may actually have a higher error ratio but have been fortunate that their errors did not fall into the serious error criteria.

5.19 Another important consideration and fairness issue in relation to naming the CSPs is the risk that identifying their involvement in certain serious errors may cause reputational or commercial damage to their businesses which could then hamper how they respond to requests for data in future. For example, the CSPs commercial imperative to protect their businesses could engender a subversive error reporting culture as I have already set out or, could hamper how they respond to requests for data in future and the extent to which they are willing to develop capabilities to support the effective and timely disclosure of data to public authorities. This is particularly crucial considering the fact that 6% (circa 30,000) of the communications data requests in 2014 were submitted in emergency situations to prevent death or injury.

5.20 Another point I took into account when considering naming the CSPs is that they are obligated by law to disclose the data. They have little or no visibility about why they are disclosing the data, they are unaware of the risk associated with the disclosure (in particular where the public authority only has that single strand of intelligence) and, they are not responsible for any action that is taken on the data. They are therefore not in a position to mitigate the impact any erroneous data may have.

5.21 In my March 2015 report I set out the considerable work that my office has undertaken to improve transparency and our commitment to better inform the public about our work. Transparency is important, but only where it improves trust or leads to greater accountability. After carefully weighting up the strengths of the arguments for and against naming on balance I concluded the arguments against were more compelling. Overall I am not convinced that the publication of the names of the individual parties would lead to greater accountability or act as a driver to improve compliance. Each error is already investigated fully and this leads to measures being implemented to prevent recurrence and to individuals who have been significantly adversely affected being informed about the mistakes, and as such there would be limited incremental benefit to the public interest in naming.

5.22 I would like to set out two caveats to my decision.

5.23 First, in cases where I establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under RIPA I shall, subject to safeguarding national security, inform the affected individual of the existence of the Investigatory Powers Tribunal (IPT) and its role, in line with the provision in paragraph 8.3 of the code of practice. In our submission[28] to the Investigatory Powers Review which was published

28 See section 3.1 http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

in December 2014 we set out some of our concerns with regard to the right to effective remedy including that the IPT can only receive a complaint from the aggrieved person who might well not be aware of the infringement; the fact that the wilful or reckless threshold is not defined and appears artificial or too high; and the lack of clarity as to whether the provision in paragraph 8.3 of the code of practice applies to CSPs. I assessed carefully each of the 17 error investigations and determined that none met the current threshold of "wilful or reckless failure".

5.24 Second, it is important that I reserve the right to name public authorities and CSPs in cases where I believe for exceptional reasons it is in the public interest to do so. For example, in cases where my office has been unable to investigate the error fully due to a lack of co-operation, or I have been unable to satisfy myself that the public authorities or CSPs concerned have taken adequate measures to prevent recurrence. I pursued a course of action in relation to one of the 17 error investigations to ensure the affected party was informed of the error because although the error was not wilful or reckless, the consequence of the error was a serious infringement of Article 10 of the European Convention on Human Rights (the right to freedom of expression). My office issued a Press Release in relation to this investigation[29].

5.25 To summarise, my decision not to name boils down to avoiding the unintended consequences of a failure of trust and confidence in organisations there to protect the public, ensuring fairness in any reporting and, ensuring the strong culture of self-reporting of errors is maintained. I am confident that our error investigations and reporting procedures achieve our objectives which are to: ensure that errors are reported; that the consequences are investigated fully; and that measures are implemented to prevent recurrence.

Summary of the serious error investigations

5.26 Annex A provides a summary of the **17** serious error investigations that were undertaken by my office in 2014. There is a table for each error which sets out whether the error was caused by a public authority, a CSP or another party; whether it was a human or technical system error; a description of the communications data acquired and; a description of the circumstances and the consequences / impact of the error.

5.27 10 of the 17 errors related to requests for internet data, predominantly cases where public authorities had sought to resolve Internet Protocol (IP) addresses[30] to individuals. IP resolution is the ability to identify who in the real world was using an IP address at a given point in time[31]. An IP address is automatically allocated by a network provider to a customer's internet connection so that communications can be routed backwards and

29 http://www.iocco-uk.info/docs/IOCCO%20Press%20Release%20re%20Vodafone%20Disclosure%20Error.pdf

30 An IP address is a numerical label assigned to each device (e.g. computer, tablet, smart phone) on the Internet. For more information on IP addresses and their allocation see https://www.ripe.net/about-us/press-centre/understanding-ip-addressing

31 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388035/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf

forwards to the customer[32].

5.28 Eight of ten 10 IP errors related to investigations into the sexual exploitation of children (for example the uploading or downloading of indecent images of children) or cases where serious concerns were raised in relation to the welfare of a child. My office has noticed an increase in the number of urgent communications data requests which relate to investigations into the sexual exploitation of children and in my March 2015 report I set out that much of the increase in the number of urgent requests is due to the police providing an enhanced emergency response to trace missing children at risk of sexual exploitation[33].

5.29 Regrettably when errors occur in relation to the resolution of IP addresses the consequences are particularly acute. An IP address is often the only line of enquiry in a child protection case (so called "single strand" intelligence), and it may be difficult for the police to corroborate the information further before taking action. Any police action taken erroneously in such cases, such as the search of an individual's house who is unconnected with the investigation or a delayed welfare check on an individual whose life is believed to be at risk, can have a devastating impact on the individuals concerned.

5.30 These errors are extremely regrettable but it is easy to see why errors are more likely to occur when resolving IP addresses than when resolving telephone numbers to individuals because of the fact that CSPs may share IP addresses between multiple customers and therefore they are re-allocated far more regularly. There are also additional complexities involved in resolving IP addresses caused by the fact that the CSPs store their data in different countries which results in a lack of consistency for example with regard to date formats and time zones.

Human Error Investigations

5.31 Errors 1-9 (see Annex A) were caused by human mistakes. Five of the nine human errors were caused by applicants making mistakes when applying for communications data in relation to internet identifiers (IP addresses or email addresses). For example, incorrectly converting the time stamp of an IP address, mistyping an email address etc. The remaining 4 errors were mistakes made by CSPs or other organisations when disclosing communications data (both telephony and internet data) to public authorities.

5.32 Whilst is inevitable that humans mistakes will occur, my office continues to highlight where more can be done to reduce the number of human errors. For example, we have made a number of recommendations for public authorities to implement measures to prevent such errors, for example, by ensuring the careful preparation and double checking of applications, by developing systems to enable communications addresses to be entered only once at the start of the application process to reduce transposition errors. My office reiterated the importance of reducing the scope for making such errors

32 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388035/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf

33 see para 7.22 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

in a circular to all Senior Responsible Officers (SROs) in September 2014 and reinforced the role of the SRO to ensure sufficient measures have been implemented to minimise the repetition of such errors[34]. These recommendations equally apply to CSPs and other organisations which disclose communications data to public authorities.

5.33 Turning to the consequences of these errors; in one case a warrant was executed at the premises of an individual unconnected with the investigation and, in a further two welfare checks were delayed on children believed to be in crisis. In three cases police visited the premises of individuals unconnected with their investigations and in the remaining three cases data was disclosed in relation to individuals who were unconnected with their investigations.

Technical System Error Investigations

5.34 Errors 10-17 (see Annex A) were caused by technical system faults. In my March 2015 report I set out that over recent years there has been a drive to update, maintain, or make more efficient CSPs disclosure processes. The Home Office have, for several years, made funds available to CSPs through the processes described in section 24(1) of RIPA, and Chapter 4 of the accompanying code, for the making of contributions towards the costs incurred by CSPs to facilitate the timely disclosure of communications data in response to requirements under RIPA. Contributions are also provided for under DRIPA where a CSP is under a requirement to retain communications data that the CSP no longer has a business requirement for.

5.35 Those funds have enabled CSPs to work with their vendors and the Home Office to develop secure disclosure systems. These secure disclosure systems have been implemented by a number of CSPs over several years. The systems aim to ensure: that requirements for data are transmitted by public authorities to the CSPs securely; that the subsequent disclosures are transferred by the CSP to the public authority securely; that an acquisition and disclosure event is produced both in the CSP and public authority which can then be audited during our inspections; the reduction of double keying within the public authority and the CSP; and to make more efficient CSPs disclosure processes.

5.36 In my March 2015 report[35] I made the point that it is crucial for such systems to be tested sufficiently prior to implementation and for quality assurance checks to be conducted regularly to ensure that the systems are functioning effectively, particularly because one technical system error can (and often does) result in a larger number of erroneous disclosures than one human error. This is one reason why technical system error investigations can take some considerable time to complete. For example error 13 (see Annex A) resulted in 862 disclosures potentially being affected. In such cases where feasible and necessary, the data requests had to be re-run by the CSP. In the case of error 13 this led to 352 erroneous disclosures being identified. This meant that 352 specific enquiries had to be made to public authority SPoCs, who in turn had to liaise

34 http://www.iocco-uk.info/docs/ErrorsCirculartoSROs.pdf
35 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

with the relevant investigating officers to inform them of the error and ascertain what action had been taken on the erroneous data and whether that action had impacted on persons not connected with the investigation. Another reason is that it sometimes takes time for the CSP to work with their vendor to identify the cause of the technical fault and to implement technical fixes. The volumes of traffic the CSPs are dealing with and the dynamic and changing technical environments make these systems complex and present constant challenges with regard to keeping the systems updated. Some of the CSPs decided to deactivate their disclosure systems or parts thereof until the technical malfunctions had been resolved.

5.37 The eight technical system errors led to four warrants being executed at premises unconnected with the investigations and in one of these instances an individual was arrested. In another case the error delayed a welfare check on a child believed to be in crisis. In one instance a person unconnected with the investigation was visited by police. The majority of these errors resulted in communications data being obtained in relation to individuals who were unconnected with those investigations. It is extremely unfortunate that in a small number of cases there were opportunities for the errors to be identified much earlier (for example, see Annex A error 10). In this particular case the investigating officer did not feedback their concerns to the SPoC after executing a warrant that did not result in evidence of the offences being committed which could have led to the data being re-checked. Not only would this have prevented a large number of subsequent erroneous disclosures, but it also would have prevented two further warrants being executed at premises related to individuals unconnected with police investigations.

Recommendations

5.38 During the error investigations my office received full co-operation. I continue to be impressed with the determination of all involved in the process to achieve and maintain high levels of compliance. Nevertheless more could be done to reduce the number of errors occurring. The following recommendations emanated from the 17 serious error investigations.

5.39 Human errors:

1 Ensure applicants, SPoCs, SROs and CSP staff dealing with disclosure requests are fully aware of the potentially serious implications of human errors.

2 Enhance capability for applicants to be able to transfer electronically (i.e. copy / paste) communications addresses (and relevant dates / times / time zones) into their applications for data where the original source information is electronically held.

3 Greater adherence to paragraph 3.68 of the code - telephone numbers (or other identifiers) to be read twice and have repeated back during urgent oral process.

4 Where there is more than one IP address related to the incident or more than one date / time, the public authority should consider resolving more than one

to enable a comparison between results.

5 Enhance the capability for SPoCs to check the source information which the applicant based their application on so the SPoC can check that the applicant has correctly interpreted the source information (for example, converted the time zones correctly).

6 Enhance capability for SPoCs to be able to transfer electronically (i.e. copy and paste) the communications address (and relevant dates / times / time zones) from the application into the CSP secure disclosure systems or a section 22(3) authorisation or section 22(4) notice.

7 Enhance capability for CSPs to be able to transfer electronically (i.e. copy and paste) the communications address (and relevant dates / times / time zones) between their systems where possible.

8 Requirement for public authority receiving the CSP disclosure (and where different, the public authority to whom that intelligence is disseminated) to check and double check all disclosures against the requirements prior to taking action.

9 Public authorities where possible should undertake research and intelligence checks to try to corroborate the disclosure prior to executing warrants.

10 Provide instruction to applicants and investigative officers to revert straight to their SPoC, or to the agency who provided the information, in cases where they might have cause to doubt the disclosure.

5.40 Technical system errors:

11 Ensure that the CSP secure disclosure systems are tested sufficiently prior to implementation and after significant updates or upgrades.

12 Ensure there is standardisation and as much consistency as possible in relation to the data entry requirements on the different CSP secure disclosure systems.

13 Requirement for SPoC to inform CSP immediately if an error is identified which might be the result of a technical system fault (even where the error has been classified as a recordable error).

14 Ensure that there are regular quality assurance audits of the CSP secure disclosure systems to identify any faults at an earlier stage.

15 Ensure that the CSPs and system vendors are aware of the potential significant consequences of system errors, that the public authorities are informed of any systems errors immediately and the errors are fixed at the earliest opportunity.

Annex A

Error Investigation 1

Error By:	Public Authority
Human or Technical:	Human
Cause:	Applicant applied for data on the incorrect email address.
Data Acquired:	Subscriber information on email address. Subscriber information relating to the Internet Protocol (IP) address identified from the email address subscriber.
Description:	A public authority sought to trace the user of an email address used to groom a young girl as part of a protracted investigation into the sexual exploitation of children. The user of the email address was in contact with the victim over social media. The applicant applied for data on the email address but missed out an underscore. The subscriber information (relating to the wrong email address) showed an IP address relating to the use of the email account. This IP address was resolved to determine where the email account was accessed from and a premises was identified. A package was provided to the relevant police force who executed a warrant at the premises. Computer equipment was seized during the search and immediate examination of the equipment was sought. The examination revealed no connection to the social media network of the victim. A subsequent review of the communications data application against the source email address caused the mistake to be realised.
Consequence:	A warrant was executed at the premises of an individual unconnected with the investigation.

Error Investigation 2

Error By:	Public Authority
Human or Technical:	Human
Cause:	Applicant applied for data in relation to an IP address but requested the data for the wrong time zone.
Data Acquired:	Subscriber information relating to an IP address.
Description:	A public authority was investigating a fraud by false representation. Fictitious goods were being placed online and bought by unsuspecting victims. The applicant made an application for subscriber information relating to the IP address associated with the fraudulent online transactions in order to identify the premises from which the offences had occurred. The applicant had the IP address and the date and time it had been used by the offender. The CSP required the date / time stamp to be converted from Pacific Standard Time (PST) to Greenwich Mean Time (GMT). The applicant made a mistake during the conversion. In this instance the raw data (2/7/2014 3:13:46 PM) required a three stage conversion: 1. month/day into day/month = 7/2/2014 2. time into 24 hour clock = 15:13:46 3. PST into GMT (+8) = 23:13:46 The applicant completed stage 1 correctly. At stage 2 they overlooked the PM and logged the time as 03:13:46. At stage 3 they added eight hours to the incorrect time which meant their request was twelve hours out. Data relating to the user of the IP address at 11:13:46 (instead of 23:13:46) was applied for and this resolved to a premises in an adjoining county. Police visited the premises but, having a named suspect, quickly identified that the person had no connection to the suspect.
Consequence:	Police visited the premises of an individual unconnected with the investigation.

Error Investigation 3

Error By:	Public Authority
Human or Technical:	Human
Cause:	Applicant applied for data in relation to an IP address but requested the data for the wrong time.
Data Acquired:	Subscriber information relating to an IP address.
Description:	An organisation had serious concerns for the wellbeing of a child who had contacted them via the internet and referred the case to a public authority using the public authority's referral form. The referral form detailed a series of nine IP addresses used by the same child during previous contacts. The applicant sought to resolve the IP address for the most recent contact to identify the premises and locate the child. The referral form requires the organisation to provide the time and date they captured the IP address as well as the specific time and date relating to the contact with the child. The applicant mistakenly acquired data relating to the capture time, rather than the actual time of the email contact and this resolved to a premises that was visited by police. No children lived at the premises and the mistake was realised. The applicant subsequently submitted an application for the correct time, identified the correct premises which was subsequently visited by police and fortunately the child was found safe and well.
Consequence:	Police visited the premises of an individual unconnected with the investigation. Delayed welfare check on a child believed to be in crisis.

Error Investigation 4

Error By:	Public Authority
Human or Technical:	Human
Cause:	Applicant applied for data in relation to 104 IP addresses but requested the data for the wrong time zone.
Data Acquired:	Subscriber information relating to 104 IP addresses.
Description:	A public authority was conducting an investigation into the sexual exploitation of children. The 104 IP addresses were used by individuals to download indecent images of children and subscriber information was acquired to identify those individuals. The applicant submitted the IP addresses in GMT when a source document advised that the time stamp should be GMT (-5). The data acquired was therefore out by five hours. An initial batch of 14 results were sent to the relevant police forces. During a subsequent operational review the time stamp mistake was noticed and the 14 police forces were immediately contacted. 10 warrants had already been executed and 4 were awaiting police action. However, in the 10 cases where warrants had been executed incriminating material had been found. The public authority reapplied for the data for the correct time period. 91 IP addresses returned exactly the same details and 10 brought back a different name and premises (but fortunately warrants had not been executed in these cases). The public authority was unable to re-apply for data in relation to the remaining three IP addresses as by that stage the data was no longer retained by the particular CSP.
Consequence:	Human error led to wrongful disclosure of data relating to 10 individuals who were unconnected with the investigation. In addition three cases where individuals had downloaded indecent images of children could not be pursued as by the time the error was identified the CSP was no longer in possession of the data.

Error Investigation 5

Error By:	Public Authority
Human or Technical:	Human
Cause:	Applicant applied for data in relation to 6 IP addresses but requested the data for the wrong time zone.
Data Acquired:	Subscriber information relating to 6 IP addresses.
Description:	In 2012 a public authority was conducting an investigation into the importation of controlled drugs. Six IP addresses related to the importation. Subscriber information was acquired on those to identify from which premises the IP addresses were used to ultimately identify the individuals involved in the importation. The investigation was not in the end pursued, but a further importation was identified towards the end of 2013 and a second investigation ensued. The 2012 data was then reviewed against the intelligence relating to the second investigation which led to enquiries being made at the premises and three witness statements being taken. In 2014 when the case was going to trial an operational review took place and the investigation team identified that the six IP addresses had been submitted in GMT and not the prevailing time zone of British Summer Time (BST). The data was therefore one hour out, throwing into question the results. One of the three witness statements was to be used in evidence. The public authority was unable to re-apply for the data as by that stage it was no longer retained by the CSPs. The Crown Prosecution Service was informed about the error, but the subsequent IOCCO investigation identified that the result intended to be used in evidence contained the lease time. The lease time proved that the IP address had stayed with the customer for several months which easily covered the one hour discrepancy.
Consequence:	In five cases the incorrect data was potentially disclosed, but the cases could not be pursued as by the time the error was identified the CSPs were no longer in possession of the data.

Error Investigation 6

Error By:	Other Party
Human or Technical:	Human
Cause:	An organisation provided a public authority with indistinct information which caused data to be acquired in relation to an IP addresses for the wrong time.
Data Acquired:	Subscriber information relating to an Internet Protocol (IP) address.
Description:	An organisation had serious concerns about the wellbeing of a child who was in contact with them via the internet and referred the details verbally to the relevant public authority. The organisation provided one IP address with two dates and times/ The first date / time related to when the child had contacted the organisation, but the second actually related to when the organisation had captured the contact (which was a more recent time). This was not made clear by the organisation and as a result the public authority sought to resolve the IP address that they thought represented the most recent contact time. The data was acquired and disseminated to the relevant police force. The police force undertook a welfare visit at the identified premises and found no children present. A subsequent check of the data identified the error. The IP address was resolved subsequently for the actual contact time and this provided a different premises but in the same force area. The same police officer visited the second address and found no children at that address either. A hoax was suspected as there was open Wi-Fi at both premises.
Consequence:	Potential delayed welfare check on a child believed to be in crisis which was ultimately determined to be a hoax.

Error Investigation 7

Error By:	Communication Service Provider (CSP)
Human or Technical:	Human
Cause:	CSP disclosed subscriber information in relation to the wrong telephone number when resolving an IP address to an account holder.
Data Acquired:	Subscriber information relating to an IP address.
Description:	An organisation had serious concerns about the wellbeing of a child who was in contact with them via the internet and referred the case to the relevant public authority. The public authority sought to resolve the IP address to locate the child. The CSP resolved the IP address to a telephone number linked to the internet account and then made a mistake when acquiring the subscriber information on the telephone number. This led to the wrong subscriber data (name and postal address relating to the telephone number) being disclosed by the CSP. The data was passed to the relevant police force; officers visited the premises and found no children living there. The result was rechecked by the CSP who identified the error. The CSP subsequently disclosed the correct data, the relevant police force visited the premises and fortunately the child was found safe and well.
Consequence:	Delayed welfare check on a child believed to be in crisis.

Error Investigation 8

Error By:	Communication Service Provider (CSP)
Human or Technical:	Human
Cause:	CSP disclosed historic subscriber information relating to a telephone number instead of the current subscriber.
Data Acquired:	Subscriber information connected to a telephone number.
Description:	An application was made by a public authority for the current subscriber details relating to a telephone number connected to an investigation into witness intimidation. The result disclosed by the CSP provided the historic subscriber. Based on this data police visited the premises identified and established the occupant was unconnected with their investigation, albeit they disclosed that they had been the subscriber to that telephone number 4 years earlier. The CSP rechecked the result and identified that the error was caused by a human mistake.
Consequence:	Police visited the address of an individual unconnected with the investigation.

Error Investigation 9

Error By:	Communication Service Provider (CSP)*
Human or Technical:	Human
Cause:	CSP wrongly disclosed a significant volume of communications data to a public authority.
Data Acquired:	Copy bills (outgoing call data) - excess data on the requested mobile telephone (i.e. a larger time span than required), and, in addition, wrongly disclosed data on a very significant number of other telephones which were part of the same account.
Description:	A public authority was undertaking an investigation into the unlawful payment of money to public officials by journalists in exchange for confidential information. During the course of the investigation the authority applied for data that included the outgoing calls from a mobile telephone used by a journalist who was a subject to investigation. The CSP responded to the legal requirement but disclosed data in excess of that required. The data disclosed contained both excess data on the requested mobile telephone (i.e. a larger time span than that required), and, in addition, wrongly disclosed data on a very significant number of other telephones which were part of the same corporate account. This mistake was a result of a human error by the CSP and regrettably the disclosure was not checked prior to it being disclosed to the police. *This error has been reported publicly. See our press release here http://www.iocco-uk.info/docs/IOCCO% 20Press%20Release %20re%20 Vodafone%20Disclosure%20Error.pdf
Consequence:	A significant volume of communications data which by its nature was a sensitive data set was wrongly disclosed by the CSP to a public authority.

Error Investigation 10

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	An upgrade to a CSP's business systems resulted in the incorrect correlation of IP addresses to subscriber data.
Data Acquired:	Subscriber information relating to IP addresses.
Description:	In May 2014 a public authority SPoC, in an effort to locate urgently a vulnerable person, requested communications data from a CSP's secure disclosure system in order to resolve an IP address to a subscriber. The public authority's SPoC concurrently contacted the CSP by phone as the requirement was urgent and the CSP conducted a manual check and disclosed the subscriber information verbally. Before any action was taken on the information, the CSP's disclosure system returned the information and the SPoC noticed that it was different to that disclosed verbally. The CSP subsequently confirmed the manual result was in fact correct and an investigation was commenced immediately into a possible technical system error. The CSP determined that there was indeed a technical system error caused by the introduction of a new data warehouse for holding company records which stored all activity in Greenwich Mean Time (GMT) only. This was a change from how records had previously been stored (namely in the prevailing time zone – either GMT or British Summer Time (BST)). This system change which took place in early 2013 was not notified to CSP staff responsible for the retention platform used for disclosing data to public authorities. As a consequence the disclosure system still indicated the need to use the prevailing time zone and not GMT. As a result the correct BST time would be read by the system as GMT which would cause subscriber information to be disclosed relating to the user of the IP address one hour later. Therefore if the IP address had been re-allocated in that hour a different subscriber might be identified. The CSP deactivated the relevant part of their disclosure system and moved to a manual system to prevent recurrence while working with their system vendor to fix the fault. The CSP launched an investigation to identify how many other disclosures might have been affected by the system error. This identified 98 potential disclosure errors...*(continued overleaf)*

Consequence:	The public authorities who had received these potentially incorrect disclosures were all contacted and an impact assessment was carried out which revealed that: • 4 returned the same result when re-run. • 94 returned different results when re-run. Of these: • In 3 cases warrants had been executed at premises relating to individuals who were unconnected with police investigations into the sexual exploitation of children (and one individual was arrested). The first warrant was executed in September 2013 the last in May 2014. Forensic searches of all the seized computer equipment found no incriminating evidence. This lack of evidence should have been the catalyst for the police forces to question the veracity of the communications data results. Had this happened the technical system error could have been identified as early as September 2013 and this would have prevented further errors from occurring. • In 4 cases intelligence work had been conducted on the results but no further action was taken; • In 56 cases no police action was taken in relation to the data; • In 31 cases the original request returned a "nil" result and as such there was no interference with the privacy of individuals unconnected with the investigations. Nevertheless the fact a "nil" result was disclosed (when there was actually a positive result) could have hampered or misled investigations.

Error Investigation 11

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	Incorrect time zone conversion
Data Acquired:	Subscriber information relating to Internet Protocol (IP) address.
Description:	A public authority sought to resolve an IP address voluntarily disclosed to them by a CSP as having been used to upload indecent images of children. The public authority identified the CSP to whom the IP address in question was allocated to and subsequently acquired the subscriber information. The result was disseminated to the relevant police force and a warrant was executed at the premises. The attending officers decided not to make an arrest. Devices were seized and steps taken to forensically examine them as quickly as possible. No incriminating evidence was found on any of the devices. It transpired that the error was caused by a technical system fault relating to time stamp conversions on the system of the CSP that originally voluntarily provided the IP address used to upload the image. The original data was seven hours out. The result could not be re-run because the data voluntarily disclosed by the first CSP was no longer retained by the CSP.
Consequence:	Warrant executed at a premises relating to individuals unconnected with the investigation.

Error Investigation 12

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	An upgrade to a CSP system caused the incorrect results to be extracted in relation to certain data requests.
Data Acquired:	Subscriber information relating to IP addresses.
Description:	A public authority was undertaking an investigation into the uploading of indecent images of children and requested details of the account connected to the IP address used to upload the images. The disclosure was compared to an earlier request made in relation to the same unidentified suspect and due to a discrepancy the SPoC queried the results. The CSP identified that a system upgrade (a new release that allowed SPoCs to enter a date range instead of a specific time and date relating to the IP address) had caused the incorrect data to be disclosed. Immediate steps were taken to fix the system fault. The CSP deactivated the relevant part of their disclosure system and moved to a manual system to prevent recurrence. Their system vendor fixed the fault promptly. The CSP reviewed the disclosures since the upgrade and identified that a further 5 requests resulted in the incorrect data being disclosed. The public authorities affected were informed and provided with the correct data. Impact assessments were conducted to ascertain what action had been taken on the original incorrect data. These showed that in one instance a welfare check on a vulnerable young person was delayed. There was no action taken in relation to the data in the other five cases.
Consequence:	Data was acquired in six cases that related to individuals unconnected with the investigations. In one of these cases a welfare check was delayed on a child believed to be in crisis.

Error Investigation 13

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	Failure in daily updates to subscriber information being transferred from CSP's business system to secure disclosure system (for 75 days).
Data Acquired:	Subscriber information relating to telephone numbers.
Description:	In November 2014 a public authority queried a subscriber information result with a CSP because it was not what they were anticipating. The CSP investigated the issue and identified that there had been a technical failure which prevented the daily updates of changes to subscriber information in the business system being transferred to the secure CSP disclosure system. The CSP identified 862 disclosures that could potentially be affected. The public authorities were notified and asked to re-check their requests and complete an impact analysis. The subsequent investigation identified that in 354 cases the correct information was actually disclosed. The investigation ascertained that the system failure was flagged to the CSP's vendor at the time it occurred. Regrettably the vendor failed to act upon the flag. If they had, this fault would have been resolved at a much earlier stage and the number of error instances would have been reduced significantly.
Consequence:	In 352 cases the correct disclosure was different to the original disclosure: • In 304 cases there was more data available than that disclosed (connection date, upgrade details). • In 27 cases where "nil" results were returned the CSP did actually hold subscriber information. In these cases the fact that "nil" results were disclosed could have hampered or misled investigations but it did not. • In 10 cases less information was disclosed than had originally been disclosed. • In 7 cases where subscriber information had been disclosed originally the re-run requests found there to be no subscriber information. • In 4 cases the incorrect subscriber was disclosed. In 144 of the 862 cases the data was no longer retained by the CSP and so the requests could not be re-run. In 12 cases the public authority decided they should not re-run the requests as it was no longer necessary or proportionate to acquire the data.

Error Investigation 14

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	A restart of a CSP's secure disclosure system after a power down led to data being disclosed to public authorities that had not been validated.
Data Acquired:	Subscriber information relating to mobile telephone numbers.
Description:	When a backlog of requests developed on a CSP's secure disclosure system, the CSP's vendor was tasked to investigate. A power down and back up was actioned and a fault was identified and later traced to a certification issue. However during the restart of the system the CSP identified that 189 disclosures that had been awaiting manual validation had been disclosed to the relevant public authorities un-validated. Each of the data disclosures could potentially have been incorrect.
Consequence:	The subsequent investigation revealed: • In 144 cases there was additional data available to that disclosed (connection / disconnection data). • In 9 cases less information was disclosed than had originally been disclosed. • In 13 instances where "nil" results were originally disclosed the re-run results showed the phones to be unregistered prepays. • In 2 instances where "nil" results were originally disclosed the CSP did actually hold subscriber information. In these cases the fact that "nil" results were disclosed could have hampered or misled investigations but it did not. • In 21 instances the correct data was originally disclosed. The CSP worked with their system vendor to fix the fault promptly.

Error Investigation 15

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	A technical fault in a CSP's secure disclosure system led to data being disclosed to public authorities that had not been validated.
Data Acquired:	Subscriber information relating to mobile telephone numbers.
Description:	A public authority queried a subscriber data result with the CSP because they noticed a discrepancy. The CSP investigated the incident and identified a technical fault that had caused incorrect data to be disclosed. The CSP took immediate remedial action, working with their system vendor to remedy the fault. An impact analysis was carried out and it was established that 265 results had the potential to contain incorrect or excess data. The CSP deactivated the relevant part of their disclosure system and moved to a manual system until the fault was fixed by the CSP's vendor.
Consequence:	A subsequent investigation of those revealed; • 82 instances where the incorrect data was disclosed. • 34 instances where incomplete subscriber details were disclosed. • 14 instances where excess data was disclosed. • 13 instances where "nil" results were originally disclosed the re-run results showed the phones to be unregistered prepays. • 122 instances where the correct data was originally disclosed.

Error Investigation 16

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	A script devised to prevent excess traffic data from being disclosed was not included in an upgrade to the CSP's secure disclosure system.
Data Acquired:	Excess traffic data (in relation to telephone numbers that had not been requested by the public authority – so called "non target" data).
Description:	A script was devised and implemented that prevented any non target traffic data being disclosed via the CSP's secure disclosure system. This function worked effectively until an upgrade to the CSP's secure disclosure system in December 2013 removed the script. Public authorities noticed the excess data, but misinterpreted it as being inextricably linked to the data they required and therefore did not challenge why it was being disclosed. The error was noticed by the Home Office during an audit of the CSP's secure disclosure system and was fixed promptly by the CSP vendor. The CSP investigated the error and identified that 207 disclosures had been made via the system after the upgrade and had resulted in excess data (non target data) being disclosed.
Consequence:	Excess data disclosed to the public authorities that they had not requested (and which had not been authorised).

Error Investigation 17

Error By:	Communication Service Provider (CSP)
Human or Technical:	Technical
Cause:	Failure of CSP's secure disclosure system to cancel requests for data that were no longer required.
Data Acquired:	Service use and traffic data
Description:	A public authority sought traffic data from a CSP's secure disclosure system to assist them to locate a high risk missing person. In this instance the missing person was found prior to the data being disclosed and as a result the SPoC cancelled the data requirement as it was no longer necessary or proportionate. There was a fault in the cancellation process on the CSP's secure disclosure system and as a result the request was not cancelled and the data was subsequently disclosed by the CSP. Following an investigation by the CSP 91 further results were identified that had been disclosed after the public authorities had cancelled the requests. It is pertinent to note that a number of these cases were urgent and due to the speed of disclosure in such cases there would not have been sufficient time to cancel the requirements. The CSP worked with their system vendor to fix the fault promptly.
Consequence:	Of the 91: • 74 (82%) had been cancelled as the data was no longer required • 17 (18%) had been cancelled due to the applicant or SPoC discovering that they had made an error by requesting the data (for example applied for data on the incorrect number).

ISBN 978-1-4741-2323-5