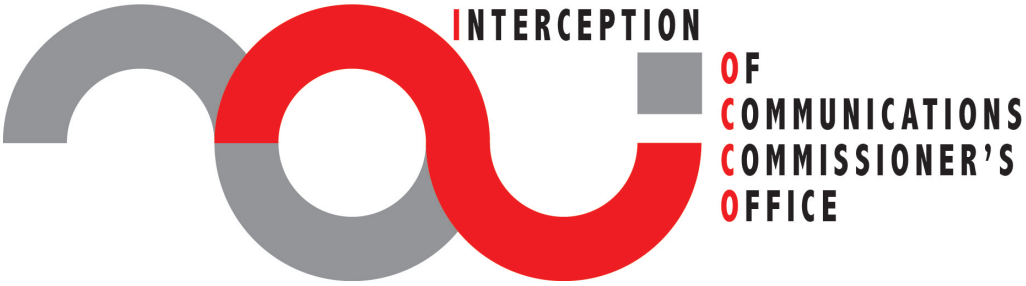


Evidence for the Investigatory Powers Review

5th December 2014

Contents

4. Transparency

- Statistical requirements that should apply – communications data
- Statistical requirements that should apply – interception
- Transparency - Public authorities
- Transparency - Oversight bodies

5. Summary of points for the review to consider

Annex A - Enhanced Statistical Requirements under Chapter 2 of Part I of RIPA

1. Introduction

1.1 During the debates considering the Data Retention and Investigatory Powers Bill, the Home Secretary announced to Parliament that the Reviewer of Counter-terrorism Legislation[1] is to lead a review before the General Election, of -

- the capabilities and powers required by law enforcement and the security intelligence agencies; and,
- the regulatory framework within which those capabilities and powers should be exercised.

1.2 This paper is the written contribution from the Interception of Communications Commissioner's Office (IOCCO) to the review.

1.3 We propose to comment on the following areas of policy -

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

1.4 We have sought to draft this paper in plain language to make it accessible to any person with an interest in the subjects being discussed. However, this paper sets out our observations about the law relating to the interception of communications, the retention, acquisition and disclosure of communications data and how this intrusive material is used once obtained. Inevitably, some legal and technical language has been used but we have tried our very best to properly explain the cause and effect.

1.5 Finally, thank you to the Independent Reviewer for allowing IOCCO extra time to finalise our submission.

[1] See https://terrorismlegislationreviewer.independent.gov.uk/

2. Effectiveness of current statutory oversight arrangements

2.1 The creation of the oversight regime

2.1.1 The debates in Parliament in March 2000, considering the then Regulation of Investigatory Powers Bill, are a good starting point in which to contextualise the current workings of the Regulation of Investigatory Powers Act 2000 ("the Act") and the oversight process. Parliament greatly expanded the role of the Interception of Communications Commissioner[2] ("the Interception Commissioner") from what was initially set out in earlier law, the Interception of Communications Act 1985, which was limited to conduct by the few agencies and relating only to interception.

2.1.2 The introduction of the Act set a legal process for the acquisition and disclosure of communications data by public authorities[3] within the United Kingdom that Parliament determined should be able to undertake the acquisition of communications data -

> Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):
>
> *"At present, the Data Protection Act safeguards are fairly lax, and have been made tighter only through voluntary co-operation between the telecoms industry and law enforcement. There is currently no independent oversight. The Bill places oversight of the use of this power under the remit of the interception of communications commissioner, which will give greater guarantees to the citizen than those that exist under the present arrangements".*

[2] See section 8 of the Interception of Communications Act 1985
[3] See the Regulation of Investigatory Powers (Communications Data) Order 2010 which contains a list of the public authorities able to use these powers, the ranks of the persons designated to grant access and the various types of communications data they may acquire http://www.legislation.gov.uk/ukdsi/2010/9780111490341/pdfs/ukdsi_9780111490341_en.pdf

2.1.3 The Act therefore replaced a disclosure process that was undertaken under the Data Protection Act 1998 and which was administered through a series of non-statutory agreements between the various communication service providers (CSPs) and the public authorities, which included police forces, law enforcement and intelligence agencies, government departments with particular investigatory responsibilities and local authorities whose functions include those of trading standards.

2.1.4 As indicated in the debate, disclosures under the Data Protection Act 1998 did not have an oversight process and the safeguards were fairly lax; so the purpose of Chapter 2 of Part 1 of the Act was to regulate access to communications data, not to extend it[4].

2.1.5 The role of the Interception Commissioner and his Inspectors from the Interception of Communications Commissioner's Office (IOCCO) is to perform an audit. The use of the terms oversight or overseer, often applied to our role, are somewhat misleading and do not best describe what Parliament intended or what we are required to do in practice.

> Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):
>
> *"An audit team from the commissioner's office will undertake periodic inspections of each body to ensure that the power is being used responsibly. [.....]. The teams will inspect records, checking the details to ensure the necessity and proportionality of what has been requested".*

[4] See 2003 consultation paper "Access to Communications Data – Respecting Privacy and Protecting the Public from Crime" - page 10

"I used the term "audit teams'' to establish that an audit will check what is happening in practice, rather than examine every case universally. We do not anticipate the need for a substantial apparatus to carry out that task. However, we do anticipate that proper regimes, such as audits, will be put in place to check that procedures are being properly followed. We shall then be able to make judgments about the necessity and proportionality of what is being done. I should like to put the right hon. Gentleman's mind at rest about the scale of the operation. I used the word ``audit'' because we want to establish systems that will genuinely assess what is taking place".

"I wanted to lay to rest the idea that we might introduce some great bureaucratic operation, and to explain why I used the word "audit'' rather than specifying a universal method of checking".

2.1.6 We have developed those audits over the years and they are now at a significantly more mature level. Further comment is made on our audits later in this paper. Our capability has also been enhanced through our recruitment of four additional Inspectors in 2013 and 2014.

2.2 Our role within the current statutory oversight arrangements

2.2.1 The Act[5] provides for an Interception Commissioner whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter 1 (interception) and Chapter 2 (acquisition and disclosure of communications data) of Part 1 of the Act. The Interception Commissioner is now supported by a team of ten inspectors (including the Head of IOCCO) and two secretariat.

[5] See sections 57 & 58 of the Act

2.2.2 We have published information about who we are on our website[6] to enable the public to have more information about the Interception Commissioner, his team, and more importantly what we actually do –

- inspections of the nine agencies (intelligence and law enforcement agencies) who may undertake the interception of communications under an interception warrant and the four warrant granting departments[7];
- inspections of all relevant public authorities who are authorised to acquire communications data[8];
- the investigation of unintentional electronic interception (not related to trying to put into effect an interception warrant). The European Commission identified deficiencies in the way in which the Data Protection Directive and the E-Privacy Directive were transposed. As a result, the offence of unintentional electronic interception, which attracts a civil penalty, was added[9]; and,
- inspections of the interception of communications in prisons in England, Wales and Northern Ireland by non-statutory agreement. This is lawful under section 47 of the Prison Act 1952 or section 13 of the Prison Act (Northern Ireland) 1953 (prison rules) – see section 4(4) of the Act.

2.2.3 It is the duty of every person to comply with any request made by the Commissioner and to disclose or provide to the Commissioner all such documents and information as he may require carrying out his functions – see section 58(1) of the Act. This means we have full and unrestricted access to all of the information, systems and documents that we need.

[6] See http://iocco-uk.info/sections.asp?sectionID=9&type=top
[7] See Paragraphs 3.3 and 3.30-3.33 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf
[8] See Annex A of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

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

2.2.4 To carry out our functions we maintain a strategic relationship with the Communication Service Providers (CSPs) which greatly assists us to carry out thorough inspections of the requirements made of them by public authorities concerning the acquisition and disclosure of communications data and their ability to comply with warrants relating to the interception of the content of communications.

2.2.5 We also maintain a close liaison with the communications data Single Points of Contact[10] (SPoCs) within public authorities who perform a guardian and gatekeeper role ensuring that the public authorities act in an informed and lawful manner when acquiring communications data. In practice our relationships with the SPoCs and CSPs serve us well.

2.3 Examination of systems and procedures for the interception of communications

2.3.1 Our interception inspections are structured to ensure that key areas derived from Chapter 1 of Part 1 of the Act and the Code of Practice are scrutinised. A typical inspection may include the following:

- a review of the action points or recommendations from the previous inspection and their implementation;
- an evaluation of the systems in place for the interception of communications to ensure they are sufficient for the purposes of the Chapter 1 of Part 1 of the Act and that all relevant records have been kept;
- examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;

[10] See Paragraphs 3.15 to 3.21 of the Acquisition and Disclosure of Communications Data Code of Practice for more information on the role of SPoC.

- interviewing case officers, analysts, linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
- examination of the urgent oral approvals to check the process was justified and used appropriately;
- an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data;
- a review of the errors reported, including checking that the measures put in place to prevent recurrence are sufficient;
- any inquiries as directed by the Interception Commissioner. For example, in 2013 we conducted investigations into matters raised by media disclosures related to revelations stemming from Edward Snowden.
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant interception agency with a copy for the relevant Secretary of State.

2.3.2 In 2013 our office carried out 26 interception inspections. During the inspections we examined 600 interception warrants. This represents just over one third of the extant warrants at the end of the year and one fifth of the new warrants issued during the year. The total number of recommendations made during our interception inspections in 2013 was 65, an average 7 recommendations for each interception agency. More detailed information on our interception work can be found in our 2013 Annual Report[11].

[11] See Section 3 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

2.4 Examination of systems and procedures for acquiring communications data

2.4.1 Our communications data inspections are structured to ensure that key areas derived from Chapter 2 of Part 1 of the Act and the Code of Practice are scrutinised. A typical inspection may include the following:

- the supply of a pre-inspection pack (two months prior to our visit) to the head of the public authority to require information and arrange interviews with operational teams;
- a review of the action points or recommendations from the previous inspection and their implementation;
- an audit of the information supplied by the CSPs detailing the requests that public authorities have made for disclosure of data. This information is compared against the applications held by the Single Point of Contact (SPoC)[12] to verify that the necessary approvals were given to acquire the data (more on this below);
- random examination of individual applications for communications data to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;
- query based examination of applications, via interrogation of the secure auditable computer systems used by the larger public authorities, to identify trends, patterns and compliance issues in key parts of the process across large volumes of applications (more on this below);
- scrutinising at least one investigation or operation from start to end to assess whether the communications data strategy and the justifications for acquiring all of the data were proportionate;
- examination of the urgent oral approvals to check the process was justified and used appropriately;

[12] See Paragraphs 3.15 to 3.21 of the Acquisition and Disclosure of Communications Data Code of Practice for more information on the role of SPoC

- a review of the errors reported or recorded, including checking that the measures put in place to prevent recurrence are sufficient;
- any inquiries as directed by the Interception Commissioner. For example, we are in the process of conducting investigations into whether there might be institutional overuse of the powers by police forces, and, the acquisition of data to identify journalistic sources; and,
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant public authority, i.e. the Chief Constable or Chief Executive.

2.4.2 In 2013 our office conducted 75 communications data inspections. An additional 130 local authorities were inspected via the National Anti Fraud Network (NAFN) who provides a SPoC service for local authorities. In 2013, 85% of the local authorities using their powers submitted their requirements via the NAFN SPoC.

2.4.3 The length of each inspection depends on the type of public authority being inspected and their communications data usage. The inspections of the larger users, such as police forces, are conducted by at least two inspectors and take place over 3 or 4 days. The inspections of the smaller volume users are conducted by one inspector and generally last 1 day. The total number of recommendations made during our communications data inspections in 2013 was 299. More detailed information on our communications data work can be found in our 2013 Annual Report[13].

2.4.4 On a regular basis the CSPs share with us information generated by the secure auditable systems that manage their disclosures to requirements made under the Act. Those audit systems contain information such as the name of the public authority acquiring data, the URN of the request, the data description and the

[13] See Section 4 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

statutory purpose used. This information allows our inspectors to perform a back audit when inspecting public authorities to assess whether there is a corresponding authority in place and its scope.

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

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

2.4.6 An application for communications data, and whether it is necessary and proportionate, is considered on the content of the application at the time it is considered by the DP determining whether to authorise it. It is our post-authorisation or down-stream audit of what is (or just as importantly what is not) being done with the data that makes our inspections unique in bringing about more scrutiny and oversight of the process. We discuss this point in more detail in the section of this paper considering prior judicial approval.

3. Safeguards to protect privacy

In addition to the oversight by the Interception Commissioner and audit by IOCCO there are other dimensions to the safeguards that we are well placed to, and therefore should, contribute to in one way or another and we will do so in this section. Reflecting on the current oversight arrangements and the safeguards has caused us to revisit some of the basic elements of the Act. We now set out our observations about what works and, in an operational sense, what does not.

3.1 The right to effective remedy - Investigatory Powers Tribunal

3.1.1 The European Convention of Human Rights ("the Convention") has had various amendments and additions made to it over the years. Article 13 of the Convention relates to the Right to an Effective Remedy -

> *Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.*

3.1.2 The Human Rights Act 1998 (HRA) does not include Article 13 relating to the Right to Effective Remedy. We understand that at the time of enactment of the HRA the view taken was that citizens within the United Kingdom would be able to seek a remedy by pursuing an action through the civil or criminal court in relation to any breach of the Convention. There have been amendments to HRA since the initial implementation (for example the withdrawal by the United Kingdom of its derogation from the Convention which concerned the detention provisions in the Anti-terrorism, Crime and Security Act 2001) but Article 13 remains absent from the HRA.

3.1.3 The Act at section 65 sets out the role and responsibilities of the Investigatory Powers Tribunal ("the Tribunal"). The section makes explicit it is the

Tribunal that is the appropriate forum if it is a complaint from a person who is aggrieved by conduct such as the interception of their communications or the acquisition of their communications data and which a person believes to have taken place in relation to them.

3.1.4 The references to a threshold for complaints dealt with by the Tribunal in the Act appears at section 65(4) and states a person needs to be "……aggrieved by any conduct……" and section 67(4) states a Tribunal does not have to hear complaints that are "……frivolous or vexatious……" and section 65(5) indicates complaints must be relating to conduct within 1 year of the conducts occurrence. In practice, the effect is –

- the complaint to the Tribunal must be from the person aggrieved;
- a third party, such as the Interception Commissioner, IOCCO or a CSP, appear unable to have their reports acted upon by the Tribunal, as the Tribunal appear limited, in law, to respond only to a complaint from the person aggrieved;
- in practice it will be virtually impossible for the aggrieved person to ever be aware of the interception of communications due to the requirement to keep secret matters relating to the existence of a warrant and the exclusion of the product of warranted interception from legal proceedings;
- there may be circumstances when communication data may be challenged as to its admissibility in criminal trials but this does not equate to matters dealt with by the Tribunal;
- section 65(5) indicates complaints must be relating to conduct within 1 year of the conduct's occurrence; and,
- the Tribunal processes appear to deal with the actions of public authorities and therefore it is not clear if that would include investigating the circumstances when a CSP is at fault concerning the interception of the wrong communications address and / or the disclosure of the wrong communications data. In 2013 we reported that 20 percent of the

interception errors and 12.5 percent of the communications data errors were caused by CSPs.

3.1.5 The code of practice accompanying Chapter 2 of Part 1 of the Act relating to the acquisition and disclosure of communications data (at paragraph 8.3) states –

> "*Should the Commissioner 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 the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal".*

3.1.6 The threshold set out in the code of "……*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"* where it relates to the acquisition of communications data appears artificial as the Act creates no such threshold to engage the Tribunal. The code also appears to confirm that erroneous actions are restricted to those of public authorities and do not include the actions of CSP when things go wrong.

3.1.7 In practice, it is the Interception Commissioner and IOCCO who will be in possession of the information as the result of the initial inspection process and, when appropriate, through the use of the powers within section 58(1) requiring the disclosure of additional information. The consequence in practice; if IOCCO becomes aware that, for example, a police force has misused their powers to acquire communications data then the proposed course of conduct suggested in the code of practice (at paragraph 8.3) of informing the aggrieved person is a rare possibility as informing them may alert them about the investigation / operation which might

amount to an act of 'tipping off', and, may be detrimental to a successful investigation or conflict with national security requirements[14].

3.1.8 Where interception with a warrant is concerned the Act prohibits an individual from being informed that their communications have been intercepted in circumstances that if they were made aware they may seek to engage the Tribunal. The code of practice accompanying Chapter 1 of Part 1 of the Act concerning the interception of communications makes no mention of the Tribunal or its processes.

3.2 The definition of content and communications data

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

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

[14] See **DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** of 25 November 2009 amending **Directive 2002/22/EC** on universal service and users' rights relating to electronic communications networks and services, **Directive 2002/58/EC** concerning the processing of personal data and the protection of privacy in the electronic communications sector and **Regulation (EC) No 2006/2004** on cooperation between national authorities responsible for the enforcement of consumer protection laws and in particular see recital (or paragraph) 64 -
"In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach."

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

3.2.4 The definitions of service use and traffic data (see sections 21(4)(a) & (b) & section 21 (6)) of the Act are, in our view, still generally fit for purpose, albeit they can be difficult to understand without proper explanation especially when a new product is launched by a CSP i.e. which definitions apply and when. Hopefully the following paragraphs can assist to explain some of the pressing issues in this regard.

3.2.5 The recent developments of communications technology appear to be included within the current definitions of service use and traffic data and an update to the examples in the Chapter 2 of Part 1 Code of Practice needs to incorporate some more recent developments as working examples.

3.2.6 One area that does need significant attention is the ability to determine what constitutes the content of a communication within the online environment. The Act refers to content several times but content itself is never defined in the Act. Explanations, therefore, that seek to differentiate by giving a threshold of, for example, "nothing beyond the first slash" do not take account of the developments within the Internet environment (for example social media), and are, in reality not best understood by investigators or CSPs managing disclosures. By way of explanation -

http://iocco-uk.info/ is said to be communications data – i.e. "nothing beyond the first slash" whereas the following link - https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/ (which is the log-in webpage to activate access to webmail) goes well

beyond the 'first slash' and may, at first appearance, be considered to be content of a communications.

3.2.7 However, section 21(6)(b) explains that traffic data (defined in section 21(4)(a)) may include data identifying or selecting or purporting to identify or select, apparatus through which, or by means of which, the communications is or may be transmitted. This then begs the question whether the log-in webpage (no matter how many 'slashes' there are within the web addresses) is communications data or the content of a communication. Amendments to the Act need to be undertaken to define what is content and by doing so better determine that which the term communications data relates to when generated within the online environment.

3.2.8 The volumes and detail contained, especially in traffic data, are at a level not envisaged in 2000. The introduction of mobile phone networks with capacity to be able to provide access to radio & television channels, social networking and other services is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone / end user device.

3.2.9 At the time the RIP Bill was being debated in 2000, traffic data relating to the location of a mobile telephone (commonly referred to as cell-site data) indicated the cell-site linked to telephone calls and text messages. The data retention requirements developed some 8 years ago required CSPs to retain cell-site data relating to telephone calls and text messages.

3.2.10 Communications data that may be used to determine the whereabouts of a mobile phone / end user device within a network is now made up by 3 elements -

1) cell-site data associated to voice and SMS retained by the mobile CSP (as described above);
2) cell-site data associated to the mobile data access channel (aka 3G or GPRS) which may relate to social media updates, messaging, access to a television channel etc.

3) Wi-Fi data indicating specific locations (for example food outlets, transport hubs such as railway stations, service stations etc) the data for which might be retained by the mobile CSP and / or another national or local provider as part of another service (for example a hotel, tube station, airport lounge, transport carrier, shopping mall, coffee shop, restaurant etc.).

3.2.11 The amount of information collected by the provider of a communications service about the people to whom they provide a service has also increased considerably and this means that the definition of "subscriber information" potentially now covers a wider catchment of data than originally available.

3.2.12 Subscriber information means, within section 21(4)(c), information held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person that is not service use data and not traffic data. When the Act was being developed some fifteen years ago subscriber data meant little more than for example, the name of the account holder, the billing postal address, the installation address of the landline, other telephone numbers present on the account.

3.2.13 The communications industry now collects significant amounts of information about the people to whom they provide pre-pay, post-pay and more latterly free or unsubscribed services. It is best to distinguish the data collected about those persons (subscriber information) from the data the industry generate or process as part of their technical infrastructure, and note that subscriber information simply means anything the CSP collects about their customer that is not data generated by the network nor is it data within their billing systems. Customers are encouraged to manage their accounts via on-line portals / 'Apps'[15] and are likely to disclose a whole

[15] "Apps" – software applications designed to run on end user devices to perform certain tasks or give streamlined access to telecommunication services (such a messaging) or information (such as weather reports).

range of personal data, for example, their viewing preferences for online media, sexual preferences, political or religious associations etc.

3.3 Authorised access to communications data

3.3.1 The offices, ranks or positions of the Designated Persons (DPs) who grant access to communications data are listed in the Regulation of Investigatory Powers (Communications Data) Order 2010[16]. The prescribed DPs who can authorise access to subscriber data (of such detail described in the previous section), not envisaged by Parliament, is worthy of consideration because of the degree of 'privacy intrusion' within subscriber information and the risk of identifying details of an individual's life, behaviour, beliefs, that the individual might regard as being more intrusive than a list of the communications that they have made or received.

3.3.2 Furthermore, the fact that some public authorities have one level of DP to authorise different types of communications data under section 21(4), whereas others have a higher ranking DP prescribed for what are traditionally thought of as the more intrusive data sets ought to be reviewed, not least to ensure the ranks / levels are comparative across the various public authorities. For example, in local authorities a DP can authorise subscriber information or service use data if they are a Director, Head of Service, Service Manager or equivalent. Similarly in the Gambling Commission one level of DP (a Head of Department) can approve all types of communications data (subscriber information, service use data and traffic data). Whereas in a police force, an Inspector can approve subscriber information, but, service use and traffic data, traditionally thought of as more intrusive data sets, must be considered by a higher ranking officer, a Superintendent.

[16] See the Regulation of Investigatory Powers (Communications Data) Order 2010 which contains a list of the public authorities able to use these powers, the ranks of the persons designated to grant access and the various types of communications data they may acquire http://www.legislation.gov.uk/ukdsi/2010/9780111490341/pdfs/ukdsi_9780111490341_en.pdf

3.4 Interception error reporting provisions

3.4.1 There is no provision for error reporting or definition of an error in the Interception of Communications Code of Practice. This leaves the interception agencies and our office struggling with an ill-defined framework. We are satisfied that there is still a good culture of self reporting, however in 2013 we reported that our investigations had identified a lack of consistency in relation to the types of error instances that are reported. This is because different thresholds and judgments are applied by each interception agency.

3.5 The role of the Single Point of Contact (SPoC)

3.5.1 We are the only Member State within the EU that has a SPoC system for acquiring communications data – accredited individuals who are trained to an expert level in acquiring the data. The SPoC's provide a guardian and gatekeeper function and ensure that their public authority acts in an informed and lawful manner when acquiring communications data. The CSP's can refuse to comply with a notice or withdraw agreement concerning an authorisation if the conduct to acquire the data does not involve a SPoC. This system ensures that data is only required when a lawful request has been made and that the data is disclosed to a known contact within the public authority.

3.5.2 The role of the SPoC and the safeguarding function they perform is set out in the Code of Practice which accompanies Chapter 2 of Part 1 of the Act. This important safeguard is not prescribed in the Act itself. The role of those working as SPoCs needs to be included in the Act, amplified in a revised Code of Practice and further enhanced by the publication professional minimum competencies by the Home Office and College of Policing.

3.6 Requirements for CSPs to retain communications data

3.6.1 There does not appear to be a legal requirement for the Interception Commissioner or any other independent oversight body to review the implementation of section 1 of the Data Retention and Investigatory Powers Act (DRIPA) which relates to the giving of notice by a Secretary of State requiring the retention of specific communications data by a CSP. There is currently no means of redress (i.e. Tribunal) for a CSP should they consider a notice requiring the retention of communications data is or has become disproportionate and should be cancelled, and, there has been a refusal to cancel it.

3.6.2 There does not appear to be a legal requirement for the Interception Commissioner or any other independent oversight body to review whether DRIPA widens the retention requirements when compared to the Data Retention (EC Directive) Regulations 2009 which it replaced[17]. The potential widening effect of DRIPA was an area of concern expressed during the debates in Parliament.

3.7 Non-compliance in relation to requirements to intercept communications or disclose data

3.7.1 Statutory oversight, audit and where appropriate, investigation, is undertaken by IOCCO when CSPs intercept communications or disclose their communications data under the Act and this includes circumstances when they disclose in error.

3.7.2 We do not oversee, audit or report to the Prime Minster when CSPs fail or refuse to intercept communications or disclose communications data when a lawful requirement is made of them within the Act.

[17] See http://iocco-uk.info/docs/IOCCO%20response%20to%20new%20reporting%20requirements.pdf for our full response to DRIPA.

3.7.3 This is a concern now that section 4 of DRIPA amends Part 1 of the Act and makes explicit the extra-territorial reach in relation to both the interception of communications and the acquisition of communications data by adding specific provisions. The amendments to the Act introduced by DRIPA confirms that requirements for interception and the acquisition of communications data to overseas companies that are providing communications services within the United Kingdom are subject to the legislation.

3.8 The use of other powers to acquire communications data

3.8.1 Chapter 2 of Part 1 of the Act appears to provide an exclusive scheme whereby communications data can be obtained. This is reinforced by section 21(1) which states that the Chapter applies to 'any conduct' in relation to obtaining of communications data, and to the disclosure to 'any person' of such data. The approach appears consistent with paragraph 1.3 of the Code of Practice for the Acquisition and Disclosure of Communications Data, which states:

> *"Relevant public authorities for the purposes of Chapter 2 of Part 1 of the Act should not:*
>
> - *Use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data, or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, or [emphasis added]*
> - *Require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998."*

3.8.2 In plain language that means public authorities should not use other laws to obtain communications data from a postal or telecommunications operator unless that law provides explicitly for obtaining communications data.

3.8.3 Parliament recently reinforced those restrictions within the Data Retention and Investigatory Powers Act 2014 (DRIPA) at section 1(6)(a) which puts a duty on the CSP not to disclose communications data retained as a result of a requirement within section 1 of DRIPA unless it is a requirement made under Chapter 2 of Part 1 of the Act; or a court order or other judicial authorisation or warrant.

3.8.4 However, there are numerous other laws which give general information powers or provide explicit powers for obtaining communications data (such as the Social Security and Fraud Act 2001 and the Social Housing Fraud Act 2013) and cases where the data retained by the CSP is not subservient to a section 1 DRIPA requirement (for example, records a CSP has determined they need to retain as part of their business function).

3.8.5 The Protection of Freedoms Act 2012[18] requiring local authorities to seek judicial authority for communications data was implemented in November 2012. The Government, in the following year, implemented the Social Housing Fraud Act 2013 which gave provision for the acquisition of service use data and subscriber information in circumstances when the data may assist to investigate housing fraud without a requirement to gain judicial approval. The Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 allows the local authority, not Parliament, to pick which local authority employees can authorise access to the data and determine what restrictions may apply to their actions, see the "Safeguards" in the Regulations –

- *"Requests for data could only be made by an authorised officer – someone who is a local authority employee and who has been authorised by the local authority's Chief Executive or Chief Finance Officer to make requests."*

[18] Protection of Freedoms Act 2012 ttp://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

- *"A local authority would be able to impose any restrictions it wished on its authorised officer and be able to withdraw authorisation at any time."*

3.8.6 The result is a two tier process in operation within the United Kingdom when there is a need for a local authority to undertake the acquisition of communications data. For example, in circumstances where a citizen is an elderly person defrauded by a rogue trader – Trading Standards must go through the rigours set down by Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act; the accompanying code practice; the additional requirements imposed by the Protection of Freedoms Act (requiring the local authorities to seek judicial approval); and subject to oversight by IOCCO. But where the local authority is subject to fraud they can investigate a crime against themselves and do not have to comply with such rigours.

3.8.7 We are of the view that CSPs should not required by law to obtain and disclose communications data other than in cases where the relevant statutory framework expressly guarantees the substantive protections of Article 8 and Directive 2002/58/EC (Directive on privacy and electronic communications).

3.8.8 We do not oversee, audit or report to the Prime Minster the use of other laws to acquire communications data which allow the public authorities using them to engage directly with the CSPs without the use of a SPoC. The person authorising is often of lower office (rank or level) and does not have to be independent from the investigation or operation; and there is no means of redress via the Tribunal.

3.8.9 Furthermore we do not oversee, audit or report on any errors or wrongful disclosures resulting from the acquisition of data using other powers.

3.9 The use of other powers to access the content of stored communications

3.9.1 Section 2(1) of the Act defines a telecommunication system as any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. "Apparatus" for these purposes includes any equipment, machinery or device and any wire or cable.

3.9.2 Sections 2(7) and (8) explain how a communication that is being stored within a telecommunication system for the intended recipient to gain or regain access to it is said to be in the course of its transmission (for example, voicemail messages stored by the CSP). Expressed another way, stored communications are always in the course of transmission even if the intended recipient has accessed them[19]. The consequence is that stored communications have the protection of section 1 of the Act which creates a criminal offence of unlawful access.

3.9.3 Accessing the content of stored communications held by a CSP will have lawful authority under section 1(5) of the Act if it is either –

- in accordance with an interception warrant under section 5 of the Act, or,
- in exercise of any statutory power that is exercised for the purpose of obtaining information or of taking possession of any document or property.

3.9.4 Reference within section 1(5)(c) to a statutory power will include the use of a section 9 Police and Criminal Evidence Act (PACE) order-

> Standing Committee F - Tuesday 16th March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):

[19] See also R v Edmondson, Brooks & others [2013] EWCA Crim 1026

> ".....Where a communication already exists, clause 1(5)(c) would allow the police to obtain a production order for access, but future communications must be accessed through an interception warrant....."

3.9.5 CSPs now deal with significant volumes of judicial orders made under section 9 of PACE (and similar) requiring the disclosure of voicemails, text messages, information retained within online storage systems, and emails. This is conduct that was envisaged by Parliament. The Times newspaper, in an article on 20th October 2014[20], revealed that one mobile CSP was receiving 150 such requirements per month. The article made the point -

> ".....Unlike warrants for eavesdropping on live conversations, so called production orders need only the approval of a judge.....", ".....the data is stored and is available to police with a production order obtained from a judge after campaigners fear is often cursory deliberation....."

3.9.6 We can confirm there is currently no oversight or audit by IOCCO of the use of other powers to acquire stored communications (for example by way of section 9 PACE orders). Furthermore there is no oversight of any errors or wrongful disclosures resulting from the use of such other powers.

3.10 The use, retention, storage and destruction of communications data within public authorities

3.10.1 We instigate thorough audits of the processes in place for the retention, storage and destruction of intercepted material and related communications data under Chapter 1 of Part 1 of the Act, but, we have no statutory footing upon which to intervene in matters relating solely to the retention, storage, processing, and destruction of communications data acquired under Chapter 2 of Part 1 of the Act within public authorities.

[20] http://www.thetimes.co.uk/tto/news/uk/article4241503.ece

3.10.2 Our inspections confirm to us how revealing, informative and, as a consequence, highly intrusive interception and communications data are in the hands of a skilled investigator. This is balanced against the very important role the prompt and efficient interception of communications or acquisition of communications data, and, the consequent analysis plays to save life, thwart threats to national security, prevent or detect crime, and, ultimately prosecute offenders.

3.10.3 For example, taking communications data, during our inspections investigators have shared with us how they use the data to assist a victim to recall events – i.e. communications will often act as a prompt to put events into sequence. They describe how victims of bullying, harassment, nuisance & malicious communications, assault, sexual assault and attempted murder will often know the offender prior to being the victim of crime. They may have communicated with them on a regular basis - especially in the online environment. Within murder investigations the victim is, more often than not, found to have been in communication with their killer. The acquisition, collation and analysis of communications data within the boundary of an investigation or operation are a powerful tool.

3.10.4 There is an absence of consolidated guidance as to what may be done with the data outside the boundary of the justifications as to why the data was acquired in the first instance which we have broken down into simple issues –

- why, how and where is the data retained within the public authority;
- if the data is further processed beyond the reasons for its acquisition are the reasons recorded with a justification as to why;
- who may access it;
- what reviews are carried out to determine which data should be destroyed or further retained; and
- are each of these steps compliant with the Data Protection Act 1998.

3.10.5 There are further questions to be determined about what the arrangements are concerning the retention and processing of communications data relating to a victim or a witness and how their privacy is safeguarded.

3.10.6 This and other privacy safeguarding issues need to be properly considered by the heads of public authorities and those who advise them as, for example, police forces are now undertaking collaborations[21]. Those regions undertaking collaboration are sharing their capabilities and one can anticipate they will be developing processes and systems so as to bring enhanced services to their work which may include the collation of data lawfully acquired.

3.10.7 We say more about the audits that we undertake with regard to the use made of the intercepted material and communications data acquired in the next section of this paper. But it is this down-stream inspection of what was or what is, and just as importantly, what was not done with the material that makes, in our view, the IOCCO inspections unique in bringing more scrutiny to the process.

3.11 The case for prior judicial approval for interception and communications data

3.11.1 In recent months there have been many comments in the media concerning professions that handle privileged information (for example, lawyers and journalists). Comment has been made that the police should have obtained production orders authorised by judges (for example under section 9 of PACE) to obtain communications data in preference to the use of Chapter 2 of Part 1 of the Act. We launched an inquiry in early October this year in relation to the acquisition of communications data by police forces to identify journalistic sources as a result of the Interception Commissioner sharing the concerns raised about the protection of journalistic sources so as to enable a free press. Our inquiry is ongoing and we intend to report our findings early in the New Year.

[21] See Policing and Crime Act 2009 http://www.legislation.gov.uk/ukpga/2009/26/contents

3.11.2 In addition, a number of the leading organisations who defend privacy, free expression and digital rights have also put forward several principles to reform surveillance[22], one of which is "judicial not political authorisation". Many cite the practices elsewhere within the EU as being more conducive with the Convention requirements within Article 8.

3.11.3 Consequently we thought it would helpful to set out some additional information to assist in developing the debate relating to prior judicial approval for interception and communications data.

3.11.4 In 2011 the EU Commission undertook an evaluation of the Data Retention Directive (Directive 2006/24/EC) and reported their findings to the Council and European Parliament[23]. Several Member States supplied information as to what processes their law enforcement and intelligence agencies undertook to gain access to communications data. The submissions included who authorised access to communications data within their jurisdictions.

Table 1 - Access to communications data within the EU[24]

Member State	**Role of person authorising access**
Belgium	Authorised by magistrate or prosecutor
Bulgaria	Chair person of regional court
Czech Republic	*No submission made*
Denmark	Magistrate / judge
Germany	*No submission made*
Ireland	Garda Síochána - senior officer
Greece	Member of judiciary
Spain	Member of judiciary
France	Senior official in Ministry of Interior

[22] For example see https://www.dontspyonus.org.uk/org
[23] http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf
[24] See footnote 23 for source of Table 1

Italy	Public prosecutor
Cypress	Public prosecutor or judge
Latvia	Police investigators or public prosecutor
Hungary	Public prosecutor
Netherlands	Public prosecutor or investigating judge
Austria	*No submission made*
Poland	Police – senior officer
Slovakia	Public prosecutor or Police
Finland	No authorisation required for subscriber information. Judge's authority for traffic data
Sweden	*No submission made*

3.11.5 Many of the individuals cited above having a role as a public prosecutor or investigating judge may, to acquire access to communications data, grant an order for the *investigation* rather than for specific data (for example one order may authorise the acquisition of historic data and / or forward facing communications data for the investigation). These general orders might satisfy the basic necessity test, but we would question how proportionality can be judged properly under such a system. The exception to this practice appears to be limited to the United Kingdom, Ireland and France – those Member States have laws that require each acquisition of data to be considered and authorised individually. That is one of the reasons why the communications data statistics published by the EU Commission when reviewing the now defunct Data Retention Directive are misleading and not comparable – because in the UK an authorisation is necessary for each requirement of data.

3.11.6 It should also be noted that many of the Member States have a model that includes a public prosecutor who is directly involved in the "pre-trial investigation" and who may also authorise access to communications data within that investigation.

3.11.7 Prior approval of interception or acquisition of communications data would involve a judge assessing whether the case for necessity and proportionality has been made. This is obviously important, but perhaps of equal importance is to examine what was or was not done with the material after it was obtained or put another way, what conduct was undertaken and whether that conduct was foreseen by the person authorising.

3.11.8 An important element missing from the processes adopted within other jurisdictions is the absence of a formal review to reassess the proportionality of the conduct authorised and, if appropriate, the renewal or review of the warrant to intercept or the authority to acquire communications data. At the time of the application for a warrant relating to interception or the acquisition of communications data, the proportionality and collateral intrusion considerations are based at a particular point in time and, importantly, prior to any Article 8 interference being undertaken. In our view, in practice, an additional and appropriate test as to whether something is, was or continues to be proportionate to the Article 8 interference undertaken can only be obtained by scrutinising the operational conduct carried out, or put another way, the downstream use of the material acquired, for example examining –

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

3.11.9 This is what makes, in our view, the IOCCO inspections unique in bringing about scrutiny through audit within the operational environment where warranted interception and the acquisition of communications data is being used i.e. examining the Article 8 interference actually being undertaken. In a scientific sense, we test the operational hypothesis set down in the initial application that was authorised and though our observations might recommend its modification or require changes to operational practice to safeguard privacy. These are all important components when looking at the principles of necessity and proportionality and compliance with the legislation and it is crucial to examine those arrangements. If the UK moved to a prior judicial model similar to those used in the EU these key components would be lost.

3.11.10 It is also important to factor in the evidence gleaned from the prior judicial approval process that has been in place under the Protection of Freedoms Act 2012 for local authority access to communications data since November 2012. The Protection of Freedoms Act (2012) amended section 57 of RIPA to make clear that –

> *"it shall <u>not</u> be the function of the Interception of Communications Commissioner to keep under review the exercise by the relevant judicial authority…" [emphasis added]*

3.11.11 That amendment, in our view, put our inspections of local authorities on a less sound footing. We sought advice from the Home Office in relation to what action we might be able to take if we identified that, for example, a judge had inappropriately approved the acquisition of traffic data which a local authority is not permitted to obtain, or, approved a request where the necessity grounds under section 22(2) of the Act were not met; considering the fact that it is not part of the function of the Interception Commissioner to keep under review the judicial approval. This point still remains unclear.

3.11.12 We have previously reported our doubts that the introduction of a judicial approval process would lead to improved standards, or, have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data[25].

3.11.13 Only a handful of requests have been refused since November 2012 and the evidence that has been shared with IOCCO to date reinforces our view that the judicial approval process for local authorities has caused confusion, increased their operational costs (for example, in Scotland a £90.00 warranty application fee is charged by the Sheriff's Office to the local authority for each application) and produced no added benefit in seeking to better the scrutiny of applications. The level of scrutiny by the judiciary is also a concern - in one case the magistrate did not ask to see the application form which set out the necessity and proportionality justifications, or the DP's approval. The application was approved on the basis of a verbal synopsis from the applicant and the DP. It is extremely concerning that the paperwork was not examined in full to check that it had been properly authorised by the DP. In another case the magistrate approved the acquisition of traffic data which local authorities are not permitted to acquire, and in another, a request was refused and the local authority was directed to undertake what were arguably far more intrusive surveillance techniques prior to obtaining subscriber information (i.e. determining the name and address to a telephone). Many local authorities have provided reports of magistrates being unaware of the amendments to the Act and their new role, which is worrying particularly considering the Home Office gave a commitment to train magistrates to carry out this role properly.

3.11.14 Local authorities have also reported experiencing lengthy time delays in obtaining an appointment with a magistrate (for example, in the worst case 6 weeks). It is questionable after this period of time whether the necessity or proportionality justifications remain valid, notwithstanding the operational and evidence gathering opportunities that may have been lost in the intervening period.

[25] See Pages 63 and 64 of our 2012 Annual Report for more information.

3.11.15 In 2013 local authorities made 1766 of the 514,608 notices and authorisations for communications data (0.3%). There were also 2760 new interception warrants issued in 2013 in addition to numerous modifications and renewals which all required ministerial approval. Notwithstanding the logistical and cost implications of a prior judicial approval process being introduced, this section has also outlined other key points worthy of consideration –

- how to ensure proportionality is considered properly by maintaining individual authorisations;
- how to ensure there is down-stream scrutiny of the use, retention, storage and destruction of material and data;
- how to ensure a mechanism for the reporting of any errors or breaches; and,
- how to ensure adequate training.

3.11.16 Without consideration and inclusion of these key points a prior judicial approval process on its own would arguably provide fewer safeguards to protect privacy.

3.12 The case for an inspector-general or similar oversight model

3.12.1 The Act gives provision for four separate Commissioners' (the Interception Commissioner, the Intelligence Services Commissioner, the Chief Surveillance Commissioner and the Investigatory Powers Commissioner for Northern Ireland) and the Tribunal. In addition the Surveillance Camera Commissioner, the Biometrics Commissioner, the Intelligence Security Committee (ISC) and the Information Commissioner's Office (ICO) all have niche responsibilities relating to the oversight of surveillance powers.

3.12.2 There have been numerous debates on oversight reform in recent years. For example, the Justice and Security Bill green paper dated October 2011 set out a number of proposals, consultation questions, and, a possible model for an Inspector-

General[26]. The Justice and Security Act 2013 reformed the Intelligence Security Committee (ISC) and gave provision for the Prime Minister to direct the Intelligence Services Commissioner to keep under review any aspect of the functions of the Intelligence Services.

3.12.3 We understand how difficult it can be for individuals to understand the roles of the various bodies involved in overseeing the legislation concerning surveillance activity in the UK. We worked with the Information Commissioners Office (ICO) to assist them to produce the Surveillance Road Map[27] which provides an overview of who is responsible for what, and, the avenues open to individuals who wish to challenge any surveillance to which they are subjected.

3.12.4 The merging of the different RIPA Commissioners may simplify the oversight model from a public perception view. It may also assist with the consideration of the principle of proportionality – as at present for example, the Interception Commissioner looks at interception warrants and communications data applications in isolation and is not generally aware of any other activity under the Act that is authorised (for example, any directed or intrusive surveillance).

3.12.5 There may be a case for the various Commissioners' oversight to be linked to the conduct authorised and undertaken rather than being linked to a particular part of legislation as is the case now, which, in our view, can cause confusion as to who is responsible for overseeing what and when. By way of example, consider the following -

- Interception of communications -
    - the Interception Commissioner oversees and audits lawful interception of communications with a warrant[28]; whereas

[26] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228860/8194.pdf
[27] http://ico.org.uk/~/media/documents/library/Corporate/Practical_application/surveillance-road-map.pdf
[28] See sections 6 to 11 of the Act

- the Chief Surveillance Commissioner oversees and audits lawful interception without a warrant[29]; but
- no one oversees or audits the interception of stored communications when a statutory power or production order[30] is used to take possession or require it to be made available.

- Reporting of errors-
  - there is a requirement for errors to be reported to the Interception Commissioner relating to the acquisition and disclosure of communications data[31]; whereas
  - there is no requirement for errors to be reported by public authorities to the Interception Commissioner relating to conduct seeking to comply with a warrant for the interception of communications; but,
  - there is a requirement for errors to be reported by CSPs to the Information Commissioner relating to conduct seeking to comply with a warrant[32]; and
  - when CSPs report errors to the Information Commissioner[33] relating to conduct seeking to comply with a warrant they may be breaching a requirement within the United Kingdom to keep matters secret relating to warranted interception[34].

3.12.6 We maintain a working relationship with our colleagues in other oversight bodies to ensure there is no lapse in oversight or audit, but things could be more streamlined, made simpler. We believe these matters could be addressed by

[29] See conduct authorised within sections 3(1) and 3(2) of the Act
[30] See section 1(5)(c) of the Act
[31] See Chapter 6 of the Acquisition and Disclosure of Communications Data Code of Practice
[32] See **REGULATION (EC) No 1211/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office –** and in particular *Article 2* - Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)-
- "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.'
- in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the **competent national authority**.

[33] Within the United Kingdom the Information Commissioner is the "competent national authority".
[34] See section 19 of the Act – offence for unauthorised disclosure

amending the various codes of practice accompanying the Act without a need to change the Act itself.

3.12.7 Merely merging the role of the Commissioners will not address this. The reality is that a merged oversight body would still require sub-teams of experts dealing with the conduct authorised by the various parts of the legislation which is, in effect, the position now. Furthermore in our 2013 Annual Report the Interception Commissioner commented that merged or enlarged oversight would risk bringing about a bureaucratic dilution of responsibility.

3.12.8 There is no doubt that one of the most important principles of oversight is independence – independence from Parliament and independence from Government. The Interception Commissioner is a former court of appeal judge and complete independence is the hallmark of any judge. The Interception Commissioner is not swayed by any political motivation and does not set out to or seek to defend, protect or promote the public authorities that his office is charged with overseeing.

3.12.9 Another important principle of oversight is to provide assurance to the public that the activities of the public authorities being overseen are reasonable, proportionate, necessary and compliant with all legal obligations, or to report where they are not. In a later section of this paper we outline the significant measures that we have taken in the last 18 months or so to improve transparency and provide further information about our work.

4. Transparency

4.1 Statistical requirements that should apply – communications data

4.1.1 Our annual report in 2012 and, again, in 2013, referred to the inadequacy of the statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice which accompanies Chapter 2 of Part 1 of the Act. The requirement is contained in Paragraph 6.5 of the Code of Practice, but essentially the public authorities are only required to report the number of authorisations and notices (written and oral) and the number of applications rejected.

4.1.2 The statistical information required by the Code of Practice is flawed for a number of reasons, including -

- more than 1 item of data may be requested on an authorisation or notice and therefore the number of individual items of communications data requested is not reported. This figure will be higher than the number of authorisations and notices;
- the different systems in use by public authorities have different counting mechanisms for notices and authorisations. For example, one public authority may request data in relation to 3 telephone numbers on 1 notice, whereas another public authority may request the same 3 items of data on 3 separate notices. The result would be an over inflated number of authorisations and notices for the second public authority. This makes meaningful comparisons difficult; and
- it is a requirement for public authorities to report the number of applications that have been *rejected* each calendar year, but not the number of applications that were approved. Therefore it is difficult to establish accurately the percentage of applications rejected.

4.1.3 Following interest on Twitter we recently published a guide to explain the relationship between applications, authorisations, notices and items of data on our

website.[35] We have consulted with the Home Office and set out the revisions and enhancements of the statistical requirements that we believe are necessary both to assist us with our audit role, and, to better inform the public about the use which public authorities make of communications data.

4.1.4 During the debates concerning the Data Retention and Investigatory Powers Bill the Minister James Brokenshire stated the Government will be amending the code of practice on the acquisition and disclosure of communications data later this year (see Hansard 15 July 2014: Column 816)[36]. We have urged the Home Office to expedite matters to bring about early public consultation. Our statistical requirements are published in Annex A of this paper for the review to consider.

4.1.5 In our 2013 Annual Report we outlined that a number of CSPs are releasing transparency figures in relation to the communications data disclosures they make to public authorities. Although it is laudable that these CSPs are trying to improve transparency and better inform their customers about how they respect their privacy, their statistics should be treated with extreme caution as again different counting mechanisms and rules are applied which can result in misleading comparisons. In our view the statistical information should be collected by the public authorities, under required conventions and counting mechanisms to ensure that it is comparable and accurate.

4.2 Statistical requirements that should apply – interception

4.2.1 There are no statistical requirements in the interception of communications data Code of Practice. The section 19 secrecy provisions make this area challenging.

4.2.2 To date we have only reported the overall number of new warrants issued and the number of extant warrants at the end of the calendar year. It may be

[35] http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf
[36] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0004.htm

possible to breakdown the total number of warrants by statutory necessity purpose (i.e. national security, serious crime, economic well-being of the UK) without prejudicing national security, and, we believe this statistic would better inform the public as to the use of these powers. A view could be taken that it would be damaging to national security to go further than this, for example, by breaking down the number of interception warrants by agency. But of equal value is the consideration as to whether the publication of further statistics on their own actually brings about better transparency.

4.3 Transparency - public authorities

4.3.1 We have encouraged the public authorities who make use of powers under the Act to engage with and contribute to the various reviews, including this one. It is also important for the public authorities to contribute to the Code of Practice consultations. This will help to ensure the various reviews and debates are informed and evidence based.

4.3.2 The public authorities also need to think about how they can better inform Parliament and the public about why they need their powers, how they make use of their powers, and, why any additional capabilities might be required.

4.4 Transparency - Oversight bodies

4.4.1 This paper has already outlined that one of the most important principles of oversight is to provide assurance to the public. We have taken significant steps in the last 18 months or so to improve transparency and provide further information about our work including –

- Annual Report - We published more detail than ever before in our 2013 Report and recommended to the Prime Minister that there should be no confidential annex;

- Website – We publish regular press releases and information in relation to the scope (and findings) of inquiries we are undertaking, responses to legislative changes, presentations or speaking notes from events attended; detailed documents explaining more about areas of our work etc;
- Twitter feed – We tweet about our inquiries and publications and re-tweet items of interest or relevance to our work;
- Public Events – We have given written and / or oral evidence to several parliamentary select committee inquiries, the Intelligence Security Committee, various reviews of powers and Government consultations. We also regularly give speeches; and attend roundtables and panel discussions at various Government, civil society, legal and industry events.

4.4.2 We intend to continue to push the boundaries in relation to how open and transparent we can be about our work to improve public confidence and understanding and contribute to ensuring any debates are informed.

5. Summary of points for the review to consider

We have already cited the background to these points in detail within the main body of this report.

5.1 Safeguards to protect privacy

The right to effective remedy

- The current threshold of "*wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers"* appears artificial as the Act creates no such threshold to engage the Investigatory Powers Tribunal ("the Tribunal). What threshold should apply as wilful or reckless appears too high?

- At what point should a citizen be advised to engage with the Tribunal?

- Article 13 of the ECHR is absent from the Human Rights Act 1998. Whilst citizens may, in normal circumstances, be able to seek a remedy by pursuing an action through the civil or criminal courts they can only do that when in possession of certain facts. If the law prohibits certain facts being made known to them they will, in reality, rarely be in possession of sufficient information to formulate the basis of a complaint - what is the effect if a citizen is unable to gain access to effective remedy?

- Should the Act be amended to enable the Interception Commissioner to make a complaint to the Tribunal on behalf of a citizen who, in our opinion, has had their rights interfered with in a manner contravening law?

- Should the Tribunal be able to deal with complaints relating to a wrongful act by a CSP when responding to a lawful requirement by a public authority – for example, when the CSP intercepts communications or discloses communications data in error?

The definition of content and communications data

- Does the determination of what constitutes the content of a communication within the online environment require better defining within the Act?
- Does the definition of subscriber information need refining or reviewing now that it potentially covers a wider catchment of data than originally available?

Authorised access to communications data

- Does the review consider the rank / level of the prescribed Designated Persons (DPs) within public authorities to be sufficient, particularly when taking into account the detail that is now captured by the term subscriber information?
- Does the review consider that the prescribed DPs are comparable across the different public authorities?

Interception error reporting provisions

- Does the review consider that there should be an equivalent error provision in the Interception of Communications Code of Practice to that in the Communications Data Code of Practice?

The role of the Single Point of Contact (SPoC)

- Does the review consider that the role of the SPoC needs to be defined in the Act, amplified in a revised Code of Practice, and, further enhanced by the publication of professional minimum competencies by the Home Office and College of Policing?

Requirements for CSPs to retain communications data

- Does the review consider that Parliament should amend the DRIPA or the Act to include a provision that requires the Interception Commissioner to oversee, audit and report on the necessity and proportionality of notices given by Secretary of State requiring the retention of specific communications data by a CSP; and whether DRIPA widens the retention

requirements when compared to the Data Retention (EC Directive) Regulations 2009 which it replaced?

Non-compliance by CSPs in relation to requirements to intercept communications or disclose data

- Should Parliament amend the DRIPA or the Act to include a provision that requires the Interception Commissioner to oversee, audit and report on instances when CSPs, within the United Kingdom or elsewhere, fail or refuse to intercept communications or disclose communications data when a lawful requirement is made of them within the Act?

Use of other powers to acquire communications data

- Should Parliament amend the Act so as to require the Interception Commissioner to oversee, audit and report to the Prime Minster on the use of other laws to acquire communications data?

- Should Parliament go further and amend the Act to include a provision that stops the use of other laws to acquire any form of communications data?

Use of other powers to acquire the content of stored communications

- Should Parliament amend the Act to include a provision that requires the Interception Commissioner to oversee, audit and report to the Prime Minster on the use of other powers to acquire the content of stored communications (for example, the use of section 9 PACE Orders).

Use, retention, storage and destruction of the communications data acquired

- Should IOCCOs audits be extended to include the oversight of the retention, storage, processing, and destruction of communications data that have been acquired by public authorities?

- Does the review consider that there needs to be consolidated and / or additional guidance within the Code of Practice concerning the retention and

/ or further processing of communications data beyond the justifications / reasons for its acquisition using Chapter 2 of Part 1 of the Act?

The case for prior judicial approval for interception and communications data

- If the UK were to move to a prior judicial approval process;
  - Should an authorisation be required for each single data or interception requirement, or, a general authorisation be provided for an investigation?
  - How would the member of judiciary review and / or renew the authority to continue interception or the acquisition of communications data?
  - How would the use, retention, storage and destruction arrangements be scrutinised?
  - Should there be a mechanism for the reporting of any errors or breaches?

5.2 Transparency

Statistical requirements that should apply – communications data

- Does the review consider the suggested enhancements to the communications data statistics at Annex A are sufficient to meet the statistical and transparency requirements envisaged?

Statistical requirements that should apply – interception

- The section 19 secrecy provisions make this area challenging – does the review consider there is provision within the Act that we can utilise more effectively to better inform the public as to what has been done in matters relating to interception?

Transparency – public authorities

- Should public authorities do more to inform Parliament and the public about why they need their powers, how they make use of their powers, and, why any additional capabilities might be required?

Transparency – oversight bodies

- What other avenues might we (and other oversight bodies) adopt to expand our audit, probe areas of concern, bring about more transparency, and, better inform the public?

Annex A

Enhanced Statistical Requirements under Chapter 2 of Part I of RIPA

The suggested statistical requirements for the revised Code of Practice will include:

- The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data;
- The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data, which were referred back to the applicant by the SPoC for amendment, including the reason for doing so;
- The number of applications submitted to a designated person for a decision to obtain communications data, which were approved after due consideration;
- The number of applications submitted to a designated person for a decision to obtain communications data, which were rejected after due consideration, including the reason for rejection;
- The number of notices requiring disclosure of communications data;
- The number of authorisations for conduct to acquire communications data;
- The number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;
- The number of **items of communications data** sought, for each notice given, or authorisation granted[37].

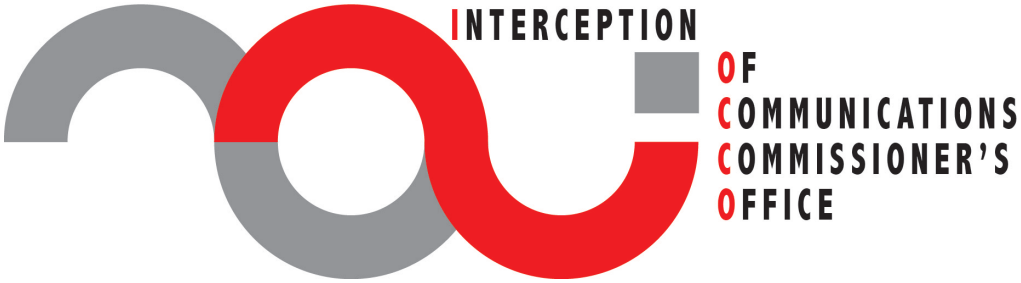
Then, for each **item of communications data** included within a notice or authorisation the public authority must also keep a record of the following:

- The Unique Reference Number (URN) allocated to the application, notice and/or authorisation;
- The statutory purpose for which the item of communications data is being requested, as set out at section 22 (2) of RIPA;

[37] One item of communications data is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of communications data.

- Where the item of communications data is being requested for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 22 (2) (b) of RIPA, the crime type being investigated;
- Whether the item of communications data is traffic data, service use information, or subscriber information, as described at section 21 (4);
- A description of the type of each item of communications data included in the notice or authorisation[38];
- Whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- Whether the data relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or Minister of religion);
- The age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;
- Where an item of data is service use information or traffic data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation;
- In the case of items of service use information or traffic data sought by means of a forward facing notice or authorisation, this will relate to the number of days of data disclosed or acquired[39];
- The CSP from whom the data is being acquired, including whether this service provider is based in the United Kingdom or elsewhere;
- The priority grading of the item of communications data;
- Whether the item of communications data is being sought by means of the urgent oral process.

[38] The data type is to include whether the data is telephone data, whether fixed line or mobile, or Internet data. Guidance on specific data types to be collected may be issued by, or sought from, IOCCO.
[39] In the case of a forward facing notice or authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. This is because a forward facing notice or authorisation will often be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the notice or authorisation may be withdrawn subsequent to that communication being made.


INTERCEPTION
OF
COMMUNICATIONS
COMMISSIONER'S
OFFICE