Senior Responsible Officer Circular (3)

Guidance on the Statistical Requirements in Paragraphs 6.5 and 6.6 of the Acquisition and Disclosure of Communications Data Code of Practice

For some time we have expressed publicly our concerns about the accuracy and reliability of the statistical requirements in the Code of Practice ("the Code") accompanying Chapter 2 of Part I of RIPA.[1] The statistical requirements lacked clarity and the counting conventions applied by police forces and other public authorities differed. This is why we made clear in successive annual reports to the Prime Minister that the statistics were only indicative of the amount of communications data acquired and must be treated with caution. We also made clear that the statistics ought not to be used inappropriately to produce league table comparisons.

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 inform the public better about the use which public authorities make of communications data powers. The revised Code which came into force on 25th March 2015 includes a more comprehensive set of statistical requirements[2]. These requirements will help to improve transparency, inform the public better about the use made of communications data powers and assist us with our inspection audits. For example, the statistics will provide information relating to the crime type for which the data was acquired, the number of refusals, the reasons for the refusals, the age of the data etc).

We required all public authorities to incorporate the new statistical requirements into their systems from April 1st 2015. We understand that the requirements have necessitated substantial changes to systems and procedures and we are grateful for the work undertaken by public authorities and workflow vendors to meet the new requirements.

The following guidance is provided to assist Senior Responsible Officers (SROs) with the annual statistical return and to provide clarity on the statistical provisions laid out in paragraphs 6.5 and 6.6 of the Code.

It is inevitable that the new statistical requirements will take time to bed in, not least because it is likely that the first annual return will include a mixture of the old statistics (between 1st January 2015 and 31st March 2015) and the new statistics (from 1st April 2015 to 31st December 2015).

We recognise the nuances and limitations of the various workflow systems, but in order to simply the process as much as possible we have not tried to account for every possible eventuality. Once we have analysed the 2015 returns we will look to provide revised guidance to ensure that going forward into 2016 the statistical requirements are refined and consistently applied.

[1] See for example Paragraphs 4.18 to 4.26 2013 Annual Report or Paragraphs 7.20 to 7.31 2014 Annual Report www.iocco-uk.info
[2] See Paragraphs 6.5 and 6.6 of the revised March 2015 Code of Practice for the Acquisition and Disclosure of Communications Data

Where a public authority has a workflow system we are now conducting detailed data analysis and query based searches during our inspections. The annual statistical returns are broader than the searches that we conduct during our inspections. For example we do not require each individual application or notice URN for the annual statistical returns (only the overall totals), but the further detail is important for inspection purposes.

Annex A (MS excel spreadsheet) issued with this circular must be used to complete your annual statistical return by **Friday 15th January 2016.** If additional assistance or advice is required to complete your return please contact IOCCO at: info@iocco.gsi.gov.uk

Code Ref	Requirement	Guidance on provision of statistics to IOCCO
Para 6.5 (A)	*The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally)*	Provide the number of applications submitted to a SPoC which includes; • All applications accepted, referred or declined by a SPoC or DP • All urgent oral • All applications by specialist departments (for example confidential unit applications based on intercept product, professional standards, counter terrorist units etc) This requirement should NOT capture; • Consequential schedules • Renewals Required dissemination format: See Annex A.
Para 6.5 (B)	*The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for* doing so.	Provide the number of times applications have been referred or declined by the SPoC including the reason for doing so which includes; • All written and oral applications (including specialist departments) • Where an application is referred more than once, each referral should be counted where possible. Required dissemination format: See Annex A. Total number of applications referred or declined grouped by reason. The following list has been produced to cover possible reasons (the list may not be exhaustive but public authorities should try wherever possible to group reasons into these categories): • Necessity - no crime / offence specified or insufficient justification of other statutory purpose • Necessity - insufficient link between crime (or other purpose), person and communications address • Proportionality – objective of acquiring data insufficiently justified including how the data will be used or analysed to meet the objective • Proportionality - insufficient justification or no rationale of date period requested

		• Proportionality – no explanation as to whether a less intrusive method of achieving objective has been considered, or tried and failed • Collateral intrusion – insufficient justification of collateral intrusion and/or how it be managed • Data no longer available, i.e. retained data over 1 year old or business systems data outside retention period • CSP unable to provide the data requested or enquiry otherwise not feasible • Applicant advised data no longer required The SPoC will obviously want to provide the applicant with more explanation to help them to address the deficiency, but the overall reason for referral or declination should ideally align to a particular category. Where there are numerous issues with one application it should be possible to refer for more than one reason (if not - common sense would suggest selecting the main reason for referral and providing further explanation of the full requirement to the applicant).
Para 6.5 (C)	*The number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were approved after due consideration.*	Provide the number of applications submitted to a DP which were approved after due consideration which includes; • All urgent oral • All applications by specialist departments (for example confidential unit applications based on intercept product, professional standards, counter terrorist units etc) • Partially authorised applications. • Approved applications which were subsequently cancelled, for any reason, prior to the acquisition of data. This requirement should NOT capture; • Renewals – because they are not counted as additional applications approved Required dissemination format: See Annex A.
Para 6.5 (D)	*The number of applications submitted to a designated person for a decision to obtain communications data, (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so.*	Provide the number of times applications have been referred or refused by the DP including the reason for doing so which includes; • All written and oral applications (including specialist departments) • Where an application is referred more than once, each referral should be counted where possible. Required dissemination format: See Annex A. Total number of applications referred or refused grouped by reason. The following list has been produced to cover possible reasons (the list may not be exhaustive but public authorities should try wherever possible to group reasons into these categories): • Necessity - no crime / offence specified or insufficient justification of other statutory purpose • Necessity - insufficient link between crime (or other purpose), person and communications address

		• Proportionality – objective of acquiring data insufficiently justified including how the data will be used or analysed to meet the objective • Proportionality - insufficient justification or no rationale of date period requested • Proportionality – no explanation as to whether a less intrusive method of achieving objective has been considered, or tried and failed • Collateral intrusion – insufficient justification of collateral intrusion and/or how it be managed • Applicant or SPoC advised data no longer required The DP may want to provide the applicant with more explanation to help them to address the deficiency, but the overall reason for referral or refusal should ideally align to a particular category. Where there are numerous issues with one application it should be possible to refer for more than one reason (if not - common sense would suggest selecting the main reason for referral and providing further explanation of the full requirement to the applicant).
Para 6.5 (E)	*The number of notices requiring disclosure of communications data (not including urgent oral)*	Total notices issued. This requirement should NOT capture; • Urgent oral notices (captured in 6.5H) Required dissemination format: See Annex A.
Para 6.5 (F)	*The number of authorisations for conduct to acquire communications data (not including urgent oral)*	Total authorisations granted. This requirement should NOT capture; • Urgent oral authorisations (captured in 6.5H) Required dissemination format: See Annex A.
Para 6.5 (G)	*The number of times an urgent application is approved orally*	Provide the total number of applications approved orally. • If a Police collaboration agreement is in place it is the duty of the public authority that closes an oral application for communications data to retain appropriate records as laid out in the CoP. Required dissemination format: See Annex A. Total number of applications approved orally.
Para 6.5 (H)	*The number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data*	Provide the total number of notices and authorisations given or granted orally. Required dissemination format: See Annex A. Total number of notices approved orally. Total number of authorisations granted orally.
Para 6.5 (I)	*The priority grading of the application for communications data, as set out at paragraph 3.5 and footnote 52 CoP.*	Total applications approved by NPGS which includes: • All written and oral applications (including specialist departments) • If grades fluctuate during the processing of an application only the initial NPGS is recorded.

		Required dissemination format: See Annex A. NPGS by application type.
Para 6.5 (J)	*Whether any part of the application 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) and if so, which profession.*	Total applications which include a requirement for data on a person who is a member of a profession that handles privileged or otherwise confidential information. Based on the belief of the applicant at the time of submission. If a person is subsequently identified as being a member of such a profession then the public authority must ensure that any further applications reflect this knowledge. Required dissemination format: See Annex A. Total number of applications by profession type.
Para 6.5 (K)	*The number of items of communications data sought, for each notice given, or authorisation granted. (Including orally).*	An item of communications data is a data requirement on a communications address or other descriptor. For example a subscriber check, a period of traffic data, a cross network search, a forward facing traffic data request. Please note: • An item remains a single item regardless of the number of enquiries made in the period of the authorisation or notice (e.g. periodic location updates are not counted individually) • Multi CSP cross network searches on a communications address are counted as a single item • A historic and live (forward facing) cell-site data requirement on a communications address is counted as one item of data for a specified period. • A subscriber check and a traffic data requirement on one communications address is to be treated as two items of data. We understand that for public authorities using workflow systems the closest equivalent to the Code definition for an "item of data" (see footnote 107) may be a "line" or "service line" of data. This may cause over inflation of figures for some types of data (such as cross network searches). We are aware of this discrepancy and will caveat appropriately the figures. Required dissemination format: See Annex A. Total number of items of communications data sought.

Code Ref	Requirement	Guidance on provision of statistics to IOCCO
Para 6.6 - For each ***item of communications data*** **(6.5K)** included within a notice or authorisation, the relevant public authority must also keep a record of the following:		
Para 6.6 (A)	*The Unique Reference Number (URN) allocated to the application, notice and/or authorisation*	Detail not required in annual statistical return.
Para 6.6 (B)	*The statutory purpose for which the item of communications data is being requested, as set out at section 22 (2) of RIPA (inc amendments by statutory instrument 2010/480)*	Total items of data by statutory purpose. Required dissemination format: See Annex A.
Para 6.6 (C)	*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.*	Items of communications data under Section 22(2)(b) by crime type. • Public authorities are advised to use the list of criminal offences in Annex A. The list may not be exhaustive but public authorities should try wherever possible to group into those categories. • Public authorities (especially those with niche statutory functions) may add offences to the list where necessary. • Public authorities should try to minimise the use of any 'other' category to ensure accuracy in reporting. Required dissemination format: See Annex A. Total number of items of data by crime type.
Para 6.6 (D)	*Whether the item of communications data is traffic data, service use information, or subscribe information, as described at section 21(4) of RIPA, and Chapter 2 of this code.*	Items of communications data by type under section 21(4), i.e. subscriber information, service use information or traffic data. Required dissemination format: See Annex A.
Para 6.6 (E)	*A description of the type of each item of communications data included in the notice or authorisation.*	Items of communications data by type (detailed). Footnote 108 of the Code sets out this requirement which appears to be at two levels. To simplify the record keeping IOCCO will only require the top level - i.e. whether the data is: • Telephony related data • Internet related data • Postal related data or • Other data (i.e. MAC address, credit card etc) Required dissemination format: See Annex A.
Para 6.6 (F)	*Whether the item of communications data relates to a victim, a witness, a complainant, or a suspect,*	The following list of data types has been provided by the NPCC. The list may not be exhaustive (see Para's 2.24 to 2.31 of the CoP for examples), however public authorities should try to ensure there is no repetition:

	next of kin, vulnerable person or other person relevant to the investigation or operation.	• Victim • Complainant • Witness • Vulnerable person (other than victim) • Next of kin • Suspect (may be further broken down by suspect: known, suspect: to identify, suspect: to trace) • Associate • Other (mandatory – please specify) Required dissemination format: See Annex A.
Para 6.6 (G)	*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.*	Total number of communications data items by 'age' category. The age of an item of data is identified as the period between the date of approval and the start date of the period required. Required dissemination format: See Annex A. Group by 'age' categories – e.g. less than 1 day, 1-7 days, 8-14 days, 15-30 days, 31-90 days, 91-120 days, 121-240 days, 241-365 days, over 365 days. For example if data is requested between 1st January 2015 and 5th February 2015 is approved by a DP on 1st June 2015 the age of the data will fall in the 121-240 days category. Note: These categories were selected by the workflow vendor which the majority of larger volume users are operating on. It is likely that we will change the date categories (reduce and align to 3 month periods) from January 2016 and further guidance will be provided by IOCCO.
Para 6.6 (H)	*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*	Total number of days of data sought by 'day' category. Please note this requirement does not include subscriber data. Where forward facing data is required the period sought (and authorised) should be counted. Required dissemination format: See Annex A. Group by 'day' categories – e.g. less than 1 day, 1-7 days, 8-14 days, 15-30 days, 31-90 days, 91-120 days, 121-240 days, 241-365 days, over 365 days. Note: These categories were selected by the workflow vendor which the majority of larger volume users are operating on. It is likely that we will change the date categories (reduce and align to 3 month periods) from January 2016 and further guidance will be provided by IOCCO.
Para 6.6 (I)	*The CSP from whom the data is being acquired.*	Total number of items of communications data requested by CSP. Required dissemination format: See Annex A.

Note: The Interception of Communications Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest or prejudicial to national security (Paragraph 6.8 of the Code).