Discovery
EXPLORE YOUR WORLD™

BY COURIER/ELECTRONIC MAIL

29.04.2019
To,
Advisor (B&CS)
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg,
Old Minto Road,
New Delhi – 110 002

Dear Sir,

Re: Submissions to Telecom Regulatory Authority of India ("TRAI") in response to the Consultation on The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual

At the outset, we would like to thank the Authority for giving us an opportunity to tender our views on the "The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual".

With regard to the present consultation process, we hereby submit that we have perused the "Issues related to The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual". We hereby submit our comments as attached in the Annexure. The said comments are submitted without prejudice to our rights and contentions, including but not limited to our right to appeal and/ or any such legal recourse or remedy available under the law and equity.
The same are for your kind perusal and consideration.

Yours Sincerely,

Ms. Mansha Shukla

Director – Legal Affairs South Asia
Discovery Communications India

Encl: As above

Discovery Communications India
(A Private Company with Unlimited Liability)

Registered Office
125-B, Som Datt Chamber-1
5 Bhikaji Cama Place,
New Delhi-110066, India
T: +91 11 41647135
F: +91 11 46032870

Regional Office
Building No - 9, Tower A,
9th Floor, DLF Cyber City,
Gurugram - 122 002, Haryana, India
T: +91 124 4349100
F: +91 124 4349289

CIN - U74300DL 1996 ULT 082136

Re: Submissions to Telecom Regulatory Authority of India ("TRAI") in response to the "The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual"

INTRODUCTION

The three fundamental elements basis which the broadcasting industry exists are the content, distribution of channels carrying content and the reach of the channels to the end subscriber of channels. A broadcaster invests significant portion of its revenues towards creation / acquisition and production of contents to be carried by the channels. The quality of reach of content depends on the technology and infrastructure adopted by the distribution platform operators ("**DPO**").

The business of a broadcaster depends on the distribution of its content per subscriber. A broadcaster is required to raise its invoices to the DPOs for payment based on the monthly subscriber report ("MSR") received from such DPO. The broadcaster does not have a direct access to its subscribers to ascertain the active number of subscribers. A broadcaster thus entirely depends on the information collected, digitally addressable technology used, transparency in the systems of the DPO to report the monthly subscriber number to the concerned broadcaster. It is paramount that a DPO's addressable system meets all of the requirements specified in Schedule III of the Telecommunication(Broadcasting &Cable) Services Interconnection Regulations, 2017 (" Regulations") which ensures, the addressable system to be protected from instances of illegal retransmission, retransmission through un-encrypted mode and most importantly accounts the distribution of each channel per subscriber.

There have been numerous instances in the past leading to litigation on the account of manipulation of data and subscriber reports as were being provided by a DPO leading to huge loss to a broadcaster because of under-declaration of subscribers and illegal retransmission of signals to its unaccounted subscribers.

Further the technical Audits that were previously being conducted by Auditors (not being an Auditor of a Broadcaster) was only limited to a mere simple tick off against the specification without ground verification, which was more to do so for the reason that the Auditor not being engaged in the day in and day out functions of the industry, absolutely having no knowledge of verifying the data provided to a particular Broadcaster by a DPO. Therefore, without understanding the loop holes created by a DPO in its system, audits were being conducted at a macro level, limited to check marking each technical specification basis the data that were being provided by a DPO which most often were manipulated data that an auditor was unaware off.

It was thus becoming difficult for Broadcasters to prove the illegality of the Audit being conducted by an Audit Agency that provided a report based on the macro audit conducted, ticking of compliance of the Schedule III of the Regulations by a DPO. Further with the requirement of mandatory provision of signals by a Broadcaster to a DPO on request coupled with a clean audit report being provided by an Audit Agency was a major backfire on a Broadcaster, wherein the Broadcaster with its hands tied was bound to provide signals to a DPO thus leading to severe revenue leakage for a Broadcaster.

Further, the current Regulations now limit the process of Audit to be conducted by the broadcaster only once a year. Hence, in light of this, it becomes imperative, that a mutually agreeable procedure and methodology should be adopted by all stakeholders so that the same is robust and watertight to cover not only a technical audit but also a detailed methodology of conducting a commercial Audit keeping in mind the commercial interest of a Broadcaster.

Therefore, the initiation vide the present consultation paper to regulate the procedure and methodology of Audit being conducted may certainly act as a relief to the issues being faced at the time of Auditing a DPO's addressable system.

The suggestion in accordance to Discovery Communications India is being provided in response to the questions as put forward by the Ld. Authority in the present Consultation paper.

RESPONSE TO ISSUES FOR CONSULTATION

Q1. Whether it should be mandatory for every DPO to notify the broadcasters (whose channels are being carried by the DPO) for every change made in the addressable system (CAS, SMS and other related system)?

A. Yes. It should be mandatory for every DPO to notify the broadcasters (whose channels are being carried by the DPO) for every change being made in the addressable system be it CAS, SMS and other related system. Any change made in the CAS/SMS system may affect the interest of the broadcasters (whose channels are being carried by the DPO), therefore every DPO should be required to notify the broadcasters thirty (30) days in advance in order to provide an opportunity to such broadcaster to understand the requirement and impact of such change by the DPO. The notification by the DPO will help maintain transparency between the DPO and broadcaster which shall in turn reduce any discrepancies in the Monthly Subscriber Reports("**MSR**")

B. Further, it is pertinent to point out that an audit is essentially conducted to ascertain that the system configurations of the SMS and CAS system ("**systems**") which the DPO has, meets the technical and commercial requirements for distribution system since, the correct functioning of the systems results in the accurate generation of MSR which determines the revenue of the broadcaster and DPO. Hence, any minute change made in the system, may affect the technical and commercial parameters which in turn may hamper the business interest of the broadcaster. In the past there have been many instances where DPOs install new CAS or SMS systems due to operational or financial reasons without notifying the broadcaster. This can lead to ambiguity particularly in cases where such new systems have not undergone any pre-technical audit to ensure new CAS / SMS systems are fully compliant with the Regulations. A pre- technical audit helps to ensure that the system is complaint with Schedule I of the Regulations and has all the relevant functionalities available in the system to generate a genuine and correct MSR report.

C. If the Broadcaster, deems it necessary then it shall be given a right to re-audit the systems of the DPO after the change has been made. The DPO should fully cooperate with such re-audit. A request to conduct Audit by a Broadcaster for the reason of change made in the addressable system, will be an exception to Regulation 15(2) of the Regulations, wherein the cost of the Audit should be borne by the DPO.

Q2. Whether the Laptop is to be necessarily provided by the Auditee DPO or the Audit Agency may also provide the Laptop? Please provide reasons for your comment.

A. Under the Regulations, Auditors are empanelled by TRAI to ensure the transparency and impartiality in carrying out the audit of systems of the DPOs. The Audit manual should categorically provide for duties, functions and liabilities of an auditor. The Auditor must act, always, without bias and should possess excellent knowledge of addressable technology and systems. The audit must be performed by a person or persons having adequate technical training

and proficiency as an auditor and due professional care is to be exercised in the planning and performance of the audit and the preparation of the report.

B. There have been several instances in the past while the broadcasters have initiated the process of audit of DPO and DPOs have provided their own laptop with extremely slow processors deliberately, that resulted in a very time-consuming audit process. Consequently, the broadcaster's expense on conducting such audit increases manifold and the time taken to receive the audit report results in huge financial difficulty for the broadcaster, as in such cases, the broadcaster cannot raise an invoice on the DPO unless the subscriber numbers are properly audited. Hence, for this purpose, it is imperative that the Laptop should be of the Audit firm/ Auditors. There should not be any interference /involvement of a DPO or broadcaster in the laptop or processes used by an auditor during audit to avoid any instances of data tampering, influencing the audit process. Any laptop being used by the Auditor during audit should be formatted before every Audit.

C. The Audit Manual should also make it mandatory for the auditor to ensure that the auditor's report should state the following with satisfactory rationale corroborated by documentary proof:

i. Whether the auditor has sought and obtained all information and explanations which to the best of his knowledge and belief were necessary for the audit and if not, the details thereof.

ii. Whether in the opinion of the auditor, proper CAS and SMS system have been maintained by the DPO as required under the Regulations.

iii. Whether, in the opinion of the auditor, the technical and commercial reports do comply with the audit manual.

iv. Auditor's detailed observations or comments on the technical and commercial reports or matter which influence the functioning of the CAS and SMS systems.

v. any qualification, reservation or adverse remark relating to the maintenance of CAS and SMS System or fingerprinting available in the system records.

vi. whether the DPO has adequate internal controls with reference to the systems used in accordance with the Regulations;

vii. Whether these systems are fool proof and non-susceptible to any hacking, virus or threats which shall compromise the technical and commercial capabilities to generate SMS reports.

D. The Audit manual shall also include an obligation on the Auditors to state that , if an Auditor in the course of the performance of his duties as auditor, has reason to believe that a DPO or its employees/officers/directors has tampered with its systems in any manner whatsoever or concealed / suppressed a material information from the auditors during the audit , the auditor shall immediately report such matter to the concerned department in TRAI and MIB within such time and in such manner as may be prescribed in the Audit Manual.

E. To ensure that the auditor is accountable for conducting audit of every DPO, the Audit Manual shall also include penalties / punishments to be imposed on the auditors. The audit report of an

auditor is of paramount importance for both DPO and Broadcaster in conducting its business in fair, transparent and accurate manner. Therefore, Audit Manual shall prescribe for appropriate penalties to ensure that the Auditors understand their liabilities of committing an offence or conducting an audit in a manner not permitted under law. The Audit Manual shall include provisions to state that in the event that an auditor contravenes any of the provisions of the Audit Manual and the Regulations, or commits fraud, forgery, supresses material information or had knowledge of fraud/ suppression of information by DPO etc., the auditor shall be made accountable and punished with a fine on the audit firm as well as every officer of the Audit firm including imprisonment for a term as prescribed by the Learned Regulator, or with both.

Q3. Whether the configuration of laptop vide Annexure 1 is suitable? If not, please provide alternate configuration with reasons thereof.

A. The configuration of laptop vide Annexure 1 may be suitable only for a small DPO. However, with reference to conducting an Audit for larger DPOs, the configuration as provided in Annexure 1 may not suffice. Further, the output from most of the CAS systems may vary in format. Therefore, it is not advisable to set out the details of specifications about the software and tools, as the requirement may vary based on the system adopted and used by each DPO.

B. Further, it is to be noted that with constant software development and upgradation, it is not advised that a fixed configuration should be detailed in the Audit Manual in respect to the laptop/computer. There are multiple CAS platforms available for Indian market which work on specific databases. It is important to have such databases on the auditee laptop i.e. SQL / Oracle databases etc. which are required while extracting and running data dump form CAS server. SMS systems must be able to quickly create adapters using standard based XML API provided by CAS vendors

In order to facilitate the audit, the DPO shall 15 days prior to audit provide the auditor its system specifications so that the auditor is well equipped and can arrange for the requisite software and configuration as would be required for the Audit.

Q4. Do you agree with the provisions regarding seeking of TS recording and ground sample information from IBF/ NBA for verification/ checking by the Auditor?

TS recording is a very critical piece of information in the process of audit which helps the auditor to identify any kind of under-declaration of subscriber base or non-reporting of CAS Systems. Hence, it should be made mandatory to have a TS recording from the IBF/NBA for the concerned broadcaster and no audit should be conducted without such TS recording. For this purpose, we agree that IBF/NBA should be a single point of contact for the Auditors, who shall write to the concerned broadcaster before any audit begins.

Q5. Do you agree that Data Dump may be cross- checked with weekly data of sample weeks basis? If yes, do you agree with checking of random 20% sample weeks? Please support your comments with justification and statistical information.

A. Yes, Data Dump may be cross-checked with weekly data of sample weeks basis. It is further agreed that upon checking of random 20% sample weeks, for the reason, that the accountability being created would keep the DPOs in check. However, the concern that crops up in respect to collecting of weekly data of sample is the practical feasibility on the ground.

B. It is also suggested that Audit Manual should include liabilities and duties of each company/vendor who provide or manage the CAS and SMS System including for extraction of data or report. These companies/vendors should be made fully liable or accountable for their actions and systems so that the systems provided by them are fool proof and non-susceptible to tampering or manipulation by the DPO in any manner or form.

C. Furthermore, the DPOs or Broadcasters should not be present during such data extraction to prevent any manipulation or undue influence on the auditors, and the CAS/ SMS vendors may be available to resolve any technical issue. The full control of such CAS/SMS System should be given to the auditor who alone will be responsible for data extraction.

D. It is further suggested that during such data extraction, the CAS vendors should provide a super administrator password to the Auditor and temporarily disable the other existing passwords so that no one can tamper or manipulate with the data during such time period in any manner.

Q6. Do you agree with the proposed Data extraction methodology? If not, suggest alternates with reasoning thereof.

A. We agree with the Data extraction methodology, which is almost like what was already being practiced during Audits. However, despite having this methodology in place, there have been many instances in the past when the DPOs have been able to manipulate Data as were being provided. Further, the Data Extraction should also be detailed per broadcaster-wise for an effective commercial Audit, as the methodology provided is more leaned towards the technical Audit. However, in terms of commercial Audit, the methodology needs to be robust and watertight. During the data extraction process, the data extracted should be arranged broadcaster-wise coupled with the monthly subscriber reports as being submitted by the DPOs to the Broadcaster along with the sample data being collected on ground.

B. Additionally, at the time of Audit, the entire dump of data should be extracted without filters, and if with filters, should be at the discretion of the Auditor. However, the Auditor should justify with reasoning use of any filter by it.

C. Live data logs should mandatorily be extracted, and back up data extracted should be coupled with previous reports and reports submitted, to verify the authenticity. However, the back- up data and reports certainly would have the possibility of manipulation, as was previously being found. Therefore, the verification process would need to be robust and watertight. It should be the responsibility of the SMS and CAS vendors to be present at the time of the audit and help the auditor extracting the database from CAS and SMS server. Broadcasters have observed on numerous occasions during the audit that DPO's technical team are not fully qualified with complex CAS and SMS systems. This therefore delays the entire audit process risking the revenues of the broadcaster.

Q7. Do you agree with verification and reporting of city-wise, state-wise and Head-end wise subscription report? Please provide supporting reasons/ information for your comment.

A. Yes, we agree with the verification and reporting of city-wise, state-wise and Head-end wise subscription report. The report should be more detailed to include broadcaster's packages, channels, al-a-carte while simultaneously verifying the reports with field samples collected.

B. It is important to capture the migration of consumers from one platform to the other platform, as the same is only visible city wise. In case the same is not done, it will lead to under declaration of subscriber base which in turn leads to tax evasion by the DPO and loss to Broadcaster revenue.

As an Illustration: - In Lucknow there is an active base of 5 lakhs subscribers which have been distributed amongst A, B and C DPO.

JANUARY 2019 CITY WISE DPO REPORT

S. No.	DPO	Subscriber Base
1.	A	20
2.	B	15
3.	C	15
TOTAL		**50**

FEBRUARY 2019 CITY WISE DPO REPORT

S. No.	DPO	Subscriber Base
1.	A	10
2.	B	15
3.	C	15
TOTAL		**40**

The difference between the total subscriber base in the city wise report is 10 and it can be clearly seen that that DPO A has reduced its subscriber base by 10 and the same has not shifted elsewhere amongst the other DPO. Hence, the DPO A is under-subscribing the subscriber base, resulting in loss of revenue for broadcaster and tax evasion to the government.

Q8. Do you agree with the tests and procedure provided for checking covert and overt fingerprinting? Provide your comments with reasons thereof?

A. Yes, we agree with the tests and procedures provided for checking covert and overt fingerprinting. However, at the time of Audit, the Auditor should obtain schedule of all broadcasters' channels distributed by such DPO and not limited to some Broadcasters. Further, the methodology needs to be more precise in respect to the tests and procedure, as the methodology prescribed is vary random. The black listed boxes should also be made part of the testing procedure. It is further suggested that there should be different colour for multiple location and multiple colours. Covert and overt fingerprinting should not happen with change in channels or volumes. Fingerprinting should appear in a Pic in Pic mode where live audio and video is available.

Q9. Any other suggestion/ comments on the provisions or methodology proposed in the Audit Manual

The Audit manual detailing the provisions and methodology has in toto ignored the aspect of being governed under the Quality of service Regulations, 2017 (QoS), it is important that emphasis will also be laid in respect to the Audit process to note if the provisions of QoS are being strictly followed or not. It is important to cover this aspect as to the request made by a subscriber to either activate or deactivate a particular channels vide email, SMS or vide a call by a subscriber, whether such requests are being followed basis the timeline as detailed in the QoS, whether the DPO is maintaining a record of the complaints filed by the subscribers and if the said complaints

are being resolved in a timely manner, whether the customer care centres as mandated under the QoS is being complied diligently and effectively, the auditor should check the mandatory requirements of the QoS regulations with a checklist. Further, any changes in the consumer interface should be recorded by the concerned DPO to make the system transparent.

It is also suggested that the CAS and SMS vendor system if found to be compromised/tampered in any manner resulting in any incorrect technical or commercial reports then in such case, the CAS and SMS company/vendor should be penalised and blacklisted and all the DPO using their system should be asked to change the same.

Further, to curb the malpractice of the DPO under declaring the subscriber base, there should be a mechanism wherein an automated notification is sent to the concerned broadcaster whenever any new subscriber opts for their channel. This will ensure transparency and control over the revenue leakage of the broadcaster.