Discovery
EXPLORE YOUR WORLD™

BY HAND/ELECTRONIC MAIL

9th September 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: **Response to the Draft of The Telecommunication (Broadcasting & Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations 2019.**

At the outset, we would like to thank the Authority for giving us an opportunity to tender our views on the issues related to "Draft of The Telecommunication (Broadcasting & Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations 2019".

In regard to the present draft amendment, we submit that we have perused the same carefully. We hereby submit our comments attached as 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.

The same are for your kind perusal and consideration.

Yours Sincerely,

Mansha Shukla

DISCOVERY COMMUNICATIONS INDIA
NEW DELHI

Mansha Shukla
Director – Legal Affairs
Discovery Communications India

Encl: As above

Response to the Draft of the Telecommunication (Broadcasting & Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations 2019

The Telecom Regulatory Authority of India ('**TRAI**') has issued the Draft of the Telecommunication (Broadcasting & Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations 2019 dated 27.08.2019 ('**Draft Amendment**'). Discovery Communications India ('**Discovery**') would like to place for consideration of TRAI, the following submissions / observations on the Draft Amendment:

1. The business of a broadcaster depends on the distribution of its content per subscriber. A broadcaster is required to raise its invoices to the distribution platform operators ("**DPO**") for payment based on the monthly subscriber report ("**MSR**") received from such DPO. The broadcaster does not have 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 systems meet all 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 re-transmission, re-transmission through un-encrypted mode and most importantly accounts the distribution of each channel per subscriber.

2. TRAI had undertaken a consultation process to prepare the Audit Manual wherein Discovery had submitted its comments / suggestion to the same. Some of the concerns raised by Discovery related to the efficient and seamless utilization of an addressable system, and essential for an effective audit process. However, these have neither been discussed nor considered by TRAI. It would have been desirable in the interest of transparency, for TRAI to deal with these concerns of Discovery while bringing out the Draft Amendment.

   <u>Digital Rights Management Systems ("DRM")</u>

3. We understand that Schedule III of the Regulations do not provide any requirements/specifications of DRM based systems, but the Draft Amendment proposes to include and regulate the DRM and include it in the part of the Schedule III of the Regulations. We agree to this point and we welcome the decision of TRAI to incorporate this change in the said Schedule.

   Further, we also recommend adding anti-piracy safety prerequisites and other technical features in the DRM technology before providing signals to any distribution platforms. We recommend adding the following pre-requisites in DRM:-

   - DRM should have the capability to generate Internet Protocol address ("IP") or unique client identification to identify the source.
   - The IP generated as mentioned above shall have a background box so that it is readable under all video conditions.

- DRM should have the capability to stop streaming using High Definition Multimedia Interface ("HDMI") output of Tablets, Laptops or smartphones etc. ("Handheld Devices").
- Streaming more than a limit of 24 hours (Twenty-Four hours) shall not be permitted. If someone is streaming more than 24 hours it's a simple case of piracy and DRM should immediately be de-authorized and should have a feature to blacklist the subscriber.
- DRM should be able to identify & block rooted Handheld Devices immediately.
- Downloading of any content on Handled Device should not be permitted by DRM. Option for downloading any content should be disabled.
- Digital watermarking on all the channels should be possible to track the source of pirate streams.
- Wi-Fi devices like miracast, chromecast, Airplay, Mirrorcast etc. can be operated via companion devices and thus content can be watched easily via OTT platforms. In DRM there should be option to disable or restrict/block these applications so that customer is not able to screen the content using these applications.
- Geo-filtering solution should also be available in DRM.
- There should be an implementation of both geo-IP databases (lookup tables) i.e. region/country-based IP database, and VPN/anonymizer/DNS proxy database as well for actual geo-location detection. There should be an update frequency of the mentioned databases/lookup tables.
- DRM should detect open, anonymous proxies and VPN proxies and there should be provision to blacklist a specific IP address if identified as proxy.
- There should be a solution to implement verification of Credit card billing address or BIN (bank Identification number) for verifying the subscriber's geographical location.
- Geo-location verification by utilizing any of the applicable/feasible technologies such as GPS Location, wifi-triangulation, GSM triangulation, network diagnostics, etc.
- Every device shall uniquely identify and authenticate devices or users including exact processes and protocols.
- There should be a criterion to detect clone devices on the network.
- There should be a tampering resistance (e.g. secure boot, code obfuscation), detection (e.g. jailbreak, root detection) or physical deterrents (e.g. custom case) for the device and/or software.
- The DRM/CAS solution should be robust against tampering and ensuring device integrity.
- DRM should securely store keys and other secrets.
- For each type of End User Device delivering HD content, a description of security measures for end-to-end video delivery including software and hardware video paths and video output control should be there.
- A systematic approach should be prescribed for renewal, upgradation, installation of the software/firmware of the CAS/DRM system.
- There should be a confirmation on the installation of third-party applications

Additionally, for the devices that have the ability to download and/or transfer content to another device, following set of questions shall be a pre-requisite for a CAS/DRM System:-

- Whether the recorded content can be played on any other device where it was not originally downloaded/recorded? How are destination devices uniquely identified and authenticated when playing recorded content (online/offline)?
- How is the recorded/downloaded content is protected?
- What is the total number of permitted devices allowed? Do you track the frequency of device registration/de-registrations? How is this tracked? Can this be limited?

Scheduling of Audit

4. In reference to the Scheduling Clause in the said Draft Amendment, we strongly feel that there should be a gap of at least 6 (six) months between the audit of two consecutive calendar years and we are supportive of this addition to the Regulations.

Fingerprinting – Support for Overt and Covert fingerprinting in STBs

5. We strongly feel that Covert Fingerprint is a vital tool to detect piracy on the ground. In absence of this tool, if by any chance Finger Printing is disabled or blocked by the entity involved in piracy, covert Finger Printing technology will be useful to detect the card number used by such entity for carrying on piracy, so that broadcasters can switch off the signals immediately. This is especially helpful during sports events or any live feed as during such events the level of piracy increases. Therefore, we strongly recommend enforcement of covert technologies.

6. Further, we recommend that it should be made applicable all across India. TRAI should come up with a deadline for DPO's to replace their existing technologies/ STBs with covert fingerprinting technology. To curb piracy, we strongly recommend inclusion of a provision wherein it shall be mandatory for all the DPOs to upgrade the existing STBs with STBs supporting covert fingerprinting within a certain timeline as prescribed by TRAI.

Transactional capacity of CAS and SMS systems

7. It is recommended that MSOs/DPOs should increase the capacity of their systems to activate STBs seamlessly without any glitch. Low transactional capacity of MSOs/DPOs result in loss to the subscribers and broadcaster.

Watermarking of network logo by the DPO

8. The watermarking logo shall be at the time of downlinking of the Content. There has been a rise of online piracy in the industry. In the case of absence of the watermarking logo, there is possibility of manifold increase in instances of piracy. There should be a provision to retain watermarking clause and encoders currently present in the market should be directed to be replaced by encoders, which have the feature to support watermarking logo for pay channels, to get a curb on piracy.

9. Further, it is strongly recommended that every multi system operator / authorized distribution platform while seeking interconnection with the Broadcaster, shall ensure that its digital addressable system installed for the distribution of TV channels meets the digital addressable system requirements ensuring that the network watermark logo is inserted on all pay channels at encoder level itself, including DVR / PVR STBs. Further, content should also get recorded along with FP/watermarking/OSD & also should display live FP during play out.

   For example- Broadcasters providing sports content or live feed will be adversely affected if this watermarking of the logos is dodged.

   In addition to the comments / suggestions on the provisions of the Draft Regulations, Discovery would like to take this opportunity to address its concerns on the audit process, which needs to be considered along with the Draft Regulations for a complete and wholesome approach on ensuring strict compliance with the parameters of addressability and to prevent manipulation of data.

   Laptop for Audit

10. Discovery had pointed out that the Audit Manual should categorically provide the duties, functions and liabilities of an auditor who is required to act always, without bias and should possess excellent knowledge of addressable technology and systems. There have been several instances in the past where 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. This led to manifold increase in the broadcaster's expense on conducting such audit, and the time taken to receive the audit report resulting 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, 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.

11. Discovery had suggested that 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.

12. It had further been pointed out that the Audit manual should 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 should 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.

13. Discovery had suggested that 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. The Audit Manual should also ensure accountability of the auditor for discharging their functions in an objective and fair manner. In the event any auditor contravenes any of the provisions of the Audit Manual and the Regulations, or commits fraud, forgery, suppresses material information or had knowledge of fraud/ suppression of information by DPO etc., the auditor should be made accountable, and subject to such fine or other consequence as TRAI deems fit.

<u>TS Recording and ground sample information from IBF/ NBA for verification/ checking by the Auditor</u>

14. It had been pointed out that 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.

<u>Cross-checking Data Dump</u>

15. Discovery had 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.

16. 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 involved 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.

17. It was 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.

18. It is respectfully submitted that these aspects are of utmost importance for ensuring a smooth operation of the addressable system. TRAI is requested to address these aspects in an appropriate manner.

Data extraction methodology

19. Discovery had pointed out that despite having the methodology in place, there have been many instances in the past when the DPOs have been able to manipulate Data that were being provided. The Data Extraction should also be detailed broadcaster-wise for an effective commercial Audit, as the current methodology provided is primarily focused on 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.

20. 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.

21. 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. 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 or cooperative with complex CAS and SMS systems. This delays the entire audit process risking the revenues of the broadcaster.

Verification and reporting of city-wise, state-wise and Head-end wise subscription report

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

23. 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.

24. 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**"). Audit process should examine as part of its checklist, 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 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 centers as mandated under the QoS are being complied diligently and effectively. Further, any changes in the consumer interface should be recorded by the concerned DPO to make the system transparent.

25. It is also suggested that the CAS and SMS vendor system if found to be technically susceptible to tampering or manipulation to generate incorrect technical or commercial reports, then in such case, the CAS and SMS company/vendor should be blacklisted and all the DPO using their system should be asked to discontinue use of such equipment / vendor.

26. 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.