Indian Broadcasting Foundation's (IBF) response on issues for consultation raised by Telecom Regulatory Authority of India ("TRAI") in Consultation Paper dated 19-July-2019 on 'KYC of DTH Set Top Boxes' ("Consultation Paper")

At the outset, we applaud TRAI for taking initiative and bringing out the Consultation Paper. We would also like to thank TRAI for giving an opportunity to stakeholders for placing their views on the topics for discussion, as enumerated in the Consultation Paper. With the substantial growth in the active subscriber base of DTH platforms (which is estimated to be approximately 72.44 million in March 2019), it has become imperative that a robust KYC or e-KYC procedure gets established so as to try and mitigate the potential dangers of piracy and loss of revenue.

The Digitisation of the cable and satellite broadcast industry, and the TRAI introduced MRP-based interconnect and tariff regulatory regime relies on the access to subscriber information and the capability to identify the subscriber and the subscriber base. Also, the delivery of the broadcast TV channel to the consumer is managed through a value-chain which involves the content creator, broadcaster and the distributor (the DPO and the Local Cable Operator), all of which stakeholders have respective requirements to enable access at the subscribers choice. These requirements, include the undeterred and secure transmission of the content and the broadcast TV channels. Hence, at the outset, we highlight that the issues addressed in the Consultation Paper and recommendations should not be restricted to DTH Set Top Boxes but also extend to Set Top Boxes of other DPOs. In this era of internet access, simple e-KYC or OTP based verification is not a difficult or costly affair, thus KYC stipulations for STBs ought to be introduced on an immediate basis.

In view of the above, our responses on various issues raised for discussion by TRAI in the Consultation Paper are appended below. We believe that there is substantial merit in our point of view presented below and accordingly, we request TRAI to consider the same at the time of taking a decision on implementation of KYC or e-KYC of DTH STBs.

1. **Is there a need for KYC or e-KYC of DTH Set Top Boxes to address the concern raised by MIB in their letter mentioned in paragraph 1.5 of this consultation paper? Give your answer with justification.**

   (a) We note that in the Consultation Paper, TRAI has referred to letters dated 27-December-2018 and 26-Mar-2019 received from Ministry of Information & Broadcasting's ("MIB") however, copies of the said letters have not been appended with the Consultation Paper. As such, our response to the issue is based on our understanding of concerns gathered by us from the background given in the Consultation Paper. In this regard, it is submitted that we are of the view that there is an absolute and an imminent need for introduction and proper enforcement of meaningful KYC or e-KYC stipulations of DTH STBs. This is necessary to inter-alia curb smuggling of DTH STBs outside of India and to bring in some level of threshold checks to counter the menace of piracy.

   (b) It is submitted that DTH STBs get rampantly smuggled to territories outside of India where they get used for illegal and unauthorized reception and/or retransmission of signals of channels. Due to such piracy, broadcasters face huge / irreparable revenue losses. Hence, there is a need for mandating KYC or e-KYC for DTH STBs to avoid smuggling of STBs overseas. DTH platforms in India are permitted to have subscribers only within the territory of India however, numerous unauthorised STBs of Indian DTH operators are reported to be active and functioning beyond the Indian territory due to the satellite footprints overspill. (For example – signals of DTH

operators intended for Indian audience are also available in Middle-East, Sri Lanka, Bangladesh, Pakistan, Afghanistan, Maldives, Nepal, Myanmar etc.).

(c) DTH platforms are mandated to confirm the address of the subscriber mentioned in the Consumer Application Form ("CAF") and activate the STB only after physical verification and installation of the STB by the DTH team. Strong KYC or e-KYC of DTH STBS would help in ensuring that DTH STBs are installed and used at such premises / locations as have been specified by the subscriber at the time of installation of DTH STBs by authorized engineers / technicians of the applicable DTH platform operator.

(d) Illegal distribution of unauthorised DTH STBs outside the territory of India amounts to piracy, financial fraud, money laundering and also unauthorised distribution of rights holders' content, affects syndication deals for the same content, entered with DPOs outside India.

(e) In case DTH STBs are found to be in use at a location other than the one specified at the time of installation, then KYC or e-KYC will enable the applicable DTH platform operator to directly approach the applicable customer to investigate why and how such DTH STB was shifted / moved to the unauthorized premises / location. This will also quicken the process of nabbing the perpetrator in case of misuse of DTH STBs.

(f) It is submitted that mere filling up of CAFs or e-CAFs by customers have not been enough in tackling piracy as there is no mechanism to ascertain veracity of information provided. It is submitted that CAFs or e-CAFs do not guarantee correctness of information contained therein. Unscrupulous operators / persons deliberately resort to filling incomplete and incorrect information in CAFs or e-CAFs, which results in feeding of incorrect data in subscriber management systems. It is submitted that incomplete and incorrect information is provided deliberately and mala fide so that unscrupulous operators / persons are able to use DTH STBs obtained by them inter-alia for illegal reception of channels outside India and/or illegal retransmission of signals. A stringent KYC or e-KYC mechanism will *inter-alia* help in identifying pirates thereby reducing any misuse. In this regard, it is submitted that though KYC or e-KYC for DTH STBs is not an end-to-end fool-proof solution to tackle unauthorized reception of channels and/or to tackle the menace of piracy and/or revenue leakages, however, it can become a potent tool to address the issues to a great extent, as a strong KYC or e-KYC mechanism will act as deterrent for misuse.

(g) Any continued failure to curtail misuse of DTH STBs outside India, will not only hurt business interests of Indian broadcasters but, will also create an impression of laxity of Indian laws to deal with issues of piracy. Failure to curtail misuse also adversely impacts rights of those players who are legitimately authorized to retransmit signals outside in their respective authorized territories outside India.

(h) As has been rightly pointed out in the Consultation Paper, the identification of a customer through KYC or e-KYC process is vital with a view to protect the customer interests by preventing fraudsters who may use the name, address and forge signature to undertake benami/illegal business activities. Identification of customers also helps to control / check financial frauds, money laundering and suspicious activities, and for scrutiny/monitoring of large value cash transactions.

(i) There has been an instance where foreign distribution platform has also resorted to instituting legal proceedings in India with an aim to seek relief against the menace of piracy. While the matter is sub-judice, however, we understand that some injunctions have been granted by courts in favour of foreign distribution platform.

(j) Additionally, at times, non-DTH DPOs within India also resort to using DTH STBs to illegally retransmit pay channels on their network. Such incidences generally occur when a broadcaster shuts down signals of its pay channels to a DPO due to non-payment of dues by such DPO. In such an event, the defaulting DPO, instead of clearing it outstanding amounts resorts to procuring multiple DTH STBs before using them to illegally retransmit the signals of those channels that have been shut down. An effective and robust KYC or e-KYC mechanism will go a long way in reducing such illegal practices.

(k) We would also like to submit that for instances where DTH STBs are caught for being used by DPOs for illegal retransmission of signals of broadcaster's channels, then the respective DTH platform whose STBs were used for such illegal retransmission of channels should be obligated to share the details of such individual subscribers with the respective broadcasters (*whose channels were retransmitted illegally*) and also to the cyber security cells for the purpose of further investigations.

2. If your answer to Q1 is in the affirmative, then what process is to be followed?

(a) We agree with the safeguard mechanisms suggested by MIB, as is mentioned in para 1.5 and 1.6 of Chapter I of the Consultation Paper.

(b) The process of identifying and verifying customers should be mandated for all DPOs.

(c) The process of registration, identification and verification through CAF, should take place by physically visiting installation address coupled with mandatorily obtaining authenticated documents related to Proof of Address and Proof of Identity (Passport, Voter ID Card, Driving Licence, Telephone Bill / Electric Bill (not older than 3 months) any other document notified by the Central Government). Activation should be initiated only after completion of all documentation.

(d) Proof of Address and Proof of Identity (through documents as identified above) of the retailer/ Seller/ Service franchisee (Installation Agency) should be made mandatory to be attached with CAF;

(e) For activation of a DPO's STB at the premises of a subscribers, the validation process may include three different OTPs getting generated and transmitted – one to the STB via b-mail *(which can be viewed on television screen connected to the STB)*, one to the subscriber's registered mobile number, and one to the mobile number of the operator's engineer / technician who visits to install and activate the STB. The STB shall only be activated with combination of these three OTPs.

(f) We submit that TRAI should also consider conducting verification exercise to ascertain whether DPOs are in compliance with QOS as well as KYC or e-KYC (as the case may be) on a periodic basis to ensure that applicable stipulations are being complied with on a continued basis. The results of such periodic audits should be put in public domain (e.g., TRAI's website) so that the same is accessible to all stakeholders. Non-compliance of QoS and/or KYC related obligations by any DPO should result in imposition of penalties on such defaulting DPOs.

3. **Whether one-time KYC is enough at the time of installation or verification is required to be done on periodic basis to ensure its actual location? If yes, what should be the periodicity of such verification?**

(a) It is submitted that One -time KYC or e-KYC should be done at the time of installation by necessary verification conducted of the subscriber address.

(b) In view of the above, it is suggested that initially the KYC or e-KYC shall be completed at the time of installation. Post initial verification, random verification can be done on a periodic basis to ensure that STB is not moved from its installation address. Periodicity of such inspection can be at such reasonable intervals as may be decided basis discussion and consultation with relevant stakeholders however, with a gap of at least three months between each visit.

(c) If a DTH STB cannot be found during physical verification at a subscriber address, then such STB should be deactivated with an *On-Screen Display*, that mentions *"update KYC* information*"*. The CAF should contain necessary terms and conditions in order to cover deactivation of STB when not found at a subscriber address.

4. **Whether KYC of the existing DTH STBs is also required to be done along with the new DTH STBs? If yes, how much time should be given for verifying the existing STBs for DTH?**

(a) KYC or e-KYC of the existing DTH STBs should also be required to be done for the same reasons as have been enumerated in our responses above.

(b) Considering the sizable number of STBs that are out there in the market, we believe that a time-period of one year should be enough from the date TRAI implements the KYC or e-KYC process..

(c) After expiry of the stipulated timeframe for completing KYC or e-KYC , recharge should be allowed only to KYC or e-KYC compliant subscribers.

5. **Whether the location-based services (LBS) needs to be incorporated in the DTH set top boxes to track its location? Will there be any cost implication? Give your response with supporting data and justification.**

(a) We fully support LBS to be incorporated in the existing DTH STBs as well as to be mandated for all new STBs of all DPOs to track location and facilitate verification. Keeping in view the growing penetration of DTH STBs and other DPOs, the security of the broadcasters' content is of paramount importance and this will also help the DPOs to minimize their own revenue loss. Pirates sell content that are gained through illegal procurement of DTH STBs at a very nominal cost, thus impacting both DTH operators' and broadcasters' revenues. Many top content providers (including studios) are hesitant to enter Indian market due to very weak content protection laws. In fact, LBS should be mandated for both DTH and HITS operators from piracy prevention perspective.

(b) It is submitted that any cost implication ought to be borne by relevant DPO. Alternatively, broadcasters ought not be compelled to provide their content to DPOs who are unable to ensure that their equipment is not capable of being misused. It surely cannot be Regulator's position that if costs for content protection are high, then content need not be protected. All existing DTH and HITS platforms are big platforms and ought not be allowed to avoid LBS on the basis of cost implication argument. The industry and specially the Regulator ought to take zero-tolerance approach when it comes to piracy prevention measures.

(c) the following options may be considered –

(i) **<u>OPTION 1</u>** – suggestion for deployment of a DTH Operator / DPO mobile Application Service (APP), on which a subscriber registers thus generating a unique user ID and password, the mobile being connected on an LBS enabled telecom network.

A) Option 1A: A unique tamper proof QR code can be permanently fixed on every STB. The DTH/DPO APP should trigger the mobile phone camera and scan the QR code and take a picture of the STB with the QR code. At the time of installation at a subscriber premises, the DTH APP must be used by the subscriber to scan the QR code and take a picture of the QR code with STB. The scanned QR code with the picture, which cannot be saved into the mobile or the DTH App, along with the mobile phones LBS information would be sent back to the DTH operator and would be used as reference ID and installation location. The QR code, once scanned through the DTH APP will successfully enable detection of the STB installed at the subscriber premises since the DTH APP is connected to an LBS enabled telecom network. The DTH APP can be used for future e-KYC on a regular basis and any deviation from the reference data can trigger the necessary corrective action such as deactivation.

B) Option 1B: Alternately, instead of fixing a tamper proof QR code on the STB, the DTH operator's head-end can trigger a unique QR code per STB for every scan instance, which will appear on the TV screen. This QR code will be valid only for a few minutes. (Similar to Aadhaar OTP). The DTH APP will enable the subscriber to scan this QR code and also take a photograph of the QR code on the TV screen. The QR code, once scanned through the DTH operator's mobile app will successfully enable detection of the STB installed at the subscriber home and the location of the STB, since the mobile phone is connected to LBS enabled telecom network. At the time of installation, the details of the STB (QR code and picture of the screen with said QR code) and the mobile phone location will get recorded at the DTH operator's end and will be used as reference data to cross check the similar data during regular e-KYC. It is essential for the subscriber to log in the DTH App with their unique user credentials created during the registration process to ensure QR code is triggered only on that subscriber's STB.

Option 1 (A) and 1(B) can be followed for monthly verification of the STB. Further, for Option 1 to be effective, all subscribers must be mandated to register for a connection through the mobile app in addition to sharing KYC details and create a unique user ID and password. The cost implication will be volume dependant which will cover the additional hardware and software for implementation of LBS at the DTH head-end and on the STB.

(ii) **Option 2 –** The DPOs STB should be enabled with mobile SIMs so that the location of the STB can be verified when required through the LBS of mobile telecom network. At the time of installation by the DPO's representative, the STB would connect to the telecom service and the geo location data through the telecom network should be saved into the DTH system as installation coordinates data and used for future reference. Each STB's LBS data can be sampled at regular intervals and compared with the reference LBS data for that STB. In case the LBS data during any sampling is noticed to be outside the predefined limits of the LBS reference data, then the corrective action such as deactivating the STB can be initiated by the DPO. The cost implication will be volume dependant which will cover the

additional hardware and software for implementation of LBS at the DPO's head-end and on the STB and mobile network data charges.

For all the options suggested above, it is suggested that it ought to be made mandatory for DTH operators to run a location test every month, share details with broadcasters and automatically deactivate the STB if any variance from the reference data is observed.

6. Any other issue relevant to KYC of DTH Set Top Boxes?

(a) While DTH STBs may be smuggled out of India, however, misuse of STBs of unscrupulous DPOs is also prevalent and needs to be curtailed. In this regard, it may be noted that STBs of other DPOs is also used for piracy of content. As such, there is no reason to restrict KYC or e-KYC process in respect of only DTH STBs, and that the same should be extended to STBs of all DPOs. All stakeholders including the Regulator need to be cognizant of the fact that content / channel piracy within India or outside, directly and/or indirectly, *inter-alia* results in reduction of funding for broadcasters and scrupulous DPOs, causes losses to public exchequer in the form of lost taxes, results in loss of job opportunities and most importantly, prevents and deprives end viewers from getting high-quality and differentiated content.

(b) In addition to introduction of robust and meaningful KYC or e-KYC process, it is submitted that:

(i) DTH and HITS operators should restrict footprints of the beams being used by them on satellites, to be focussed to the territorial limits of India. In this regard, DTH and HITS operators should be compelled to use narrow beams known as 'spot beams' to provide service by DTH operators over a narrow geographic region.

(ii) It is submitted that in any event, DTH and HITS operators should, by themselves, opt for 'spot beams' / 'focussed beams' focussed for India since, spill-over would essentially mean wastage of power and bandwidth. It may be noted that 'spot beam' not only ensures strong signal quality but also allows DTH and HITS operators to provide more channels, which can result in more revenue per subscriber.

(iii) It should be mandatory that DTH and HITS operators are compelled to adjust direction of uplinking dish to point at a satellite whose beam only serves India.

(iv) DTH operators should be directed to use CAS that would limit its users based in India to access content while denying access to users outside India. Technology to provide geographical information about end users to DTH operators is already in place and the same can be easily deployed.

(c) It is recommended that archival CAF data is converted to e- KYC. Physical CAF should be eventually replaced by e-KYC.

***