

THE TELECOMMUNICATION (BROADCASTING AND CABLE)
SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS
(AMENDMENT) REGULATIONS, 2019 (___ of 2019)
DRAFT REGULATIONS

Shri. Anil Kumar Bhardwaj,
Advisor (B&CS),
Telecom Regulatory Authority of India (TRAI),
emailed to: advbcs-2@traigov.in and
sapna.sharma@traigov.in.

Dear Sir,

Sub: Draft Telecommunication (Broadcasting and Cable)
Services Interconnection (Addressable Systems
(Amendment) Regulations, 2019.

(1.0) I refer to the draft dated 27-08-2019 seeking
and inviting written comments on the above subject
from the stakeholders by 9th September, 2019.

(2.0) I give my written comments herein. Screenshots
from TRAI's draft have been captured and inserted to
aid the comments process. Please arrange to open and
read the attached bookmarked PDF file named
"TRAI_27082019(090919)-psn.pdf"

(3.0) I thank you for providing an opportunity to
present my comments on this subject.

Yours Sincerely,

(P.S.Natarajan)

06-09-2019

Category of Comments: Individual/Member of the Public

The Comments are presented as follows...

(1.0) Clause (C) – Page 2 from TRAI’s Draft:-

Addressable Systems Requirements

(C) Conditional Access System (CAS) and Subscriber Management System (SMS):

1. The distributor of television channels shall ensure that the current version of the CAS, in use, do not have any history of hacking.

(1.1) Comments for Clause (C) – Page 2 from TRAI’s Draft:-

(a) This raises many questions. How can TRAI ensure that there is no history of hacking, by whom, and who is/are the victims of hacking, and are there any instances of reported instances of hacking to TRAI which it can make public and put it up on the website.

(b) What TRAI needs in this context must be specified to remove any misunderstanding later on besides a comprehensive definition of what constitutes “hacking” specifically targeted and to cover all transactions bearing in mind the contextual framework and background of a CAS/DTH/or similar platforms as one has to consider that these are broadcast based, satellite covered, digitally operable, one way communication, and so on. *(It is likely that “hacking” has already been defined elsewhere yet these are new vistas to be explored.)*

(2.0) Clause (C) – Pages 2 and 3 from TRAI’s Draft:-

Addressable Systems Requirements

(C) Conditional Access System (CAS) and Subscriber Management System (SMS):

(2.1) Comments for Clause (C) – Pages 2 and 3 from TRAI’s Draft:-

(a) Clauses 2 to 12 are to be welcomed in subscriber's interests if the costs are not loaded to the subscriber or passed on through increased subscription charges, channel charges or under other "Miscellaneous" heads.

(b) This particular point may kindly be borne **throughout this Draft** as otherwise it would mean repeating this issue.

(c) Additionally other provisions in this Draft that bring in good governance and system checks, audit, etc are to be welcomed without specifically referring to them here as otherwise it would mean repeating this issue.

(3.0) Clause 13(v) on Page 4 from TRAI's Draft:-

(v) List of blacklisted STBs in the system.

(3.1) Comments for Clause 13(v) on Page 4 from TRAI's Draft:-

(a) This blacklisting of STBs must only be for the specified purposes and must be laid down as decided by TRAI which Authority should define and decide all instances where "blacklisting" can be enforced. This might cover, among others, instances of illegal use, misuse, contravention of law, rules or regulations, diversionary use of signals, activation unilaterally when deactivated, non permitted use, smuggling, piracy, and so on. In other words, an "unfriendly" or "often-complaining-nuisance" subscriber cannot be blacklisted unilaterally by the MSO/DTH/Cable Operator under this provision of "Blacklisting" as the affected "blacklistee" is affected and must be given an opportunity to defend his stand, represent and clarify before such actions are finalized. As TRAI also decides whether the

blacklisting is reasonable or not it would introduce further transparency and governance with confirmed and decided blacklisted cases that can be put up on TRAI's website also.

(b) Therefore "Blacklisting" must be initiated only after TRAI's approval as and when the matter is reported to them so that they are aware of that aspect, are put on notice and obtain knowledge of that aspect.

(c) This may even be useful and crucial as in the case of involvement of allegations of smuggling that need a more thorough investigation in confirmation or to rule out such activity and cannot be decided "from the armchair" so to speak. Blacklisting arising there from can be under TRAI's supervision and TRAI is empowered to initiate action on that basis or *suo moto* take up such issues.

(d) TRAI's report to any another Central Government Agency will carry greater weight and credibility so that the Customs, Immigration, Emigration, Border check point Authorities, etc., can take action more efficiently based on TRAI's report as TRAI has sent the report to them or placed that matter before such Authorities for suitable action.

(4.0) Clauses 6, 9 and 11 under (E) on Page 6 from TRAI's Draft taken together:-

(E) Set Top Box (STB):

6. The messaging character length should be minimal 120 characters.
9. The STB must be compliant to the applicable Bureau of Indian Standards.
11. The STBs with facilities for recording the programs shall have a copy protection system.

(4.1) Comments on Clauses 6, 9 and 11 under (E) on Page 6 from TRAI's Draft taken together:-

(a) Is this minimal requirement of 120 words any technical requirement without which there would be non-functioning of the system is to be addressed and one presumes that there is no maximum word limit herein as a 120 word limit minimum is prescribed.

(b) Compliance with BIS standards as regards fingerprinting of STBs is dependent on the pre-2017 and post 2017 operational scenario. Pre-2017 covered only Overt parameters and were even not mandated then by the TRAI regulations. Pre-2017 did not cover Covert parameters. Post 2017 if it is to be made applicable, both Overt and Covert parameters must be provided in TRAI's Regulations and under the BIS Standards also. Here again this technology infusion should not be an excuse to load costs by targeting the subscriber base by increased subscription costs, channel charges, etc.

(c) In case the imported equipment are in use and already approved by say a reputed foreign agency (Let us name this as "FCA" in this example) as being electrically safe, energy efficient, radiation emission free or within limits, and so on, that has taken care of all issues, should these be re-certified by or under BIS standards and would the BIS certification be made mandatory or should they possess two or more certifications...BIS plus **FCA**...these are some of the issues that require to be addressed. Let us say that BIS standards are less demanding than **FCA**, then which would prevail...BIS or **FCA**...or if more demanding, would there be increased costs for mere compliance with BIS standards.

(d) Copy protection issue is dealt with later on under the heading of "Digital Rights Management" under

paragraphs (7.0) and (7.1) below.

(5.0) (C) 8 Page 3 and (F) 7 Page 7 from TRAI's Draft:-

8. The CAS and the SMS should be able to activate or deactivate services or STBs of at least Five percent (5%) of the subscriber base of the distributor within 24 hours.
7. The DRM and the SMS should be able to activate or deactivate services or STBs of at least 10% of the subscriber base of the distributor within 24 hours.

(5.1) Comments for (C) 8 Page 3 and (F) 7 Page 7 from TRAI's Draft:-

(a) Both related clauses are dealt in one place to avoid repetitive comments. It is indeed difficult to predict figures and specify the exact percentage on transactional capacities of CAS and SMS systems as 5% or 10%. The potential to activate or deactivate within 24 hours involves the entire subscriber base and for some major players that could run to a stupendous figure. If that entails adding additional expensive equipment to just meet a revised TRAI norm and that also, consequentially, passes on the burden to the subscriber then they should be a re-look. I would like to give an example. On a day## the CBSE website is relentlessly confronted with anxious hits and visits as the results of the Board Exams are to be announced thereby flooding and choking the servers and systems on that day, though the CBSE is well prepared to handle "normal traffic" for that given day....and this is "abnormal traffic" at one given time where multiple accesses chokes and taxes all systems....and yet the CBSE is also prepared ideally for "Result Day Traffic" also as part of its plan. (##or prior if news of impending results are announced)

(b) Are the MSO/DTH operators

* handling excessive traffic on a daily basis or
* would they be required to be well prepared for a figure that is just right on an "abnormal" day that can be predicted and factored in, or
*is it totally unlikely that there would be no such instance...then why prepare and spend money for that event, or
*it is not required on a daily basis but has to be done anyway to fulfil TRAI's norms,

and are they likely to face a situation similar to the CBSE load example scenario and can they handle that in a contingency or happening event, but need not handle it on a daily basis....in other words, the provision, the planning, and the preparedness is there, and can be scaled up, if required, but is not being deployed daily.

(c) Past records will have to be studied in order to arrive at a figure that is acceptable to the industry and even allowed on a case-by-case basis depending on the subscriber base and other factors. "One size fits all" may not be ideal but records must be used to let TRAI decide, and once TRAI decides, that should be the norm for that MSO/DTH and in prosperous times, the figure would be dynamically scaled up for any MSO/DTH based on market intelligence and TRAI's own supervisory roles as a Regulator.

(6.0) Clause 5 Page 11 from TRAI's Draft:-

framework, the authority considers that the annual Audit caused by Distributor shall be scheduled in such a manner that there is a gap of at-least two quarters between the audit of two consecutive calendar years.

(6.1) Comments for Clause 5 Page 11 from TRAI's Draft:-

(a) This is indeed a welcome step and the idea mooted

by TRAI is to space audits to such periods that are meant to avoid an illusory purpose and satisfy mere "on-paper" requirements in case the audits were to be held within shorter span of time periods.

(b) If that actually and effectively ensures and brings out the positive aspects in any audit for better governance and transparency and for better working of the system and the laws that regulate them, then that is indeed a welcome step.

**(7.0) Clause 17 from Page 13 from TRAI's Draft:-
Digital Rights Management (DRM)**

**(7.1) Comments on Clause 17 from Page 13 from TRAI's
Draft:- Digital Rights Management (DRM)**

(a) A word on Digital Rights Management (DRM). To stand tall in the Hall of Nations that support proper media content regulations, aid in piracy prevention and to protect intellectual property laws globally, DRM is important.

(b) One must realize that embedded codes have been cracked on CDs, DVDs, Blu-rays, etc and a digital film is spread worldwide even before it hits the theatre when the **threat-re** (*please note the deliberate spelling mistake here shown and the mix-up of the alphabets along with the split up word*) as "re" could also mean "regarding" as the copy-piracy threat might well lie in the preview theatres where these preview centres can be regarded as sources themselves or these are copied from other clandestine pre-release "close-and-with-access-to-content" sources. Once copied they flood the web and bleed a lot of revenue loss for the industry undermining efforts, piggy-ride on someone's else money and make more money, mock hard work, belittle risk taking, insult enterprise, ignore talent, and stifle creativity that goes behind

any film or for that matter a book, a drama or digital content that is to be afforded intellectual property protection.

(c) I am against piracy and do support all measures for effective DRM protection but somewhere along the way, when DRM and copy protection are spoken of in the same breath, we need to understand its contextual colour, background and framework, that so long as Set Top Boxes with recording facilities are allowed and are provided it is difficult to prevent copying even if it were to be stated as being copied and kept in recorded condition for "Fair and permitted use" such as

" I missed viewing the serial yesterday and am viewing it today during my spare time"....

and in order to implement a DRM/copy protection regime would it mean banning STBs with recording facilities and is it not pushing the concept a bit too far might be the question. To many this option might be impractical, unrealistic and a revenue burner when such STBs have already flooded the market and are popular, and in demand, always.

(d) Fair Non Commercial DRM compliant practices are generally allowed, very broadly put and rather imprecisely, but it is so obvious and in vogue and so easy to record content or watch any shared content or otherwise access or download content over the web.

(e) A film through a DTH operator can be copied via the STB with recording facility in HD....some make it more convenient by providing USB slots where one inserts the pen drive, USB drive or Micro SD and so on to copy. Some could just copy off the displayed TV after the signal has been "de-encrypted" fully, thanks

to the STB, which does the job of "de-crypting" the transmitted encrypted signals. Watermarks, banners, interruptions from advertisements, logos, etc make little impact here and many do not bother about these minor intrusions as they watch content happily. In fact "break-free" movies or "advertisement-free" movies or content command a higher premium capitalizing on the tolerance level and short patience fuse when a viewer is intent on watching advertisement free content and is ready and willing to pay more for this break free viewing experience.

(f)At the end of the day it would be stated by a MSO/DTH/Operator/Content Provider/ somewhat on these lines as the practice goes....

*"I, the MSO/DTH/Operator/Content Provider/have paid the film producer## for the rights to broadcast the film" and "I am providing that to my paid subscribers"
(##directly or through others##)*

.....and the subscriber having paid subscription fee to me can watch and also copy on his STB (and watch numerous times sourced from this STB till he remains a subscriber with me....We have on offer paid content also such as Video On Demand (VoD) or "Showtime" on pay-and-view basis that is time restricted or number of views restricted....

.....and if the subscriber exits from me, I, the MSO/DTH/Operator/Content Provider/ will remove the Zeetoo points on the subscriber's STB....

.....and the subscriber can longer watch that film again.... the subscriber is stuck with me... and that STB with the film recorded or lying in its copied state is totally useless to the subscriber now...."

(g)MSO/DTH/Operator/Content Provider will also inform you the occasions when your stored recordings will be lost forever...and some instances are mentioned here such as:-

- (i)when you change the pack,
- (ii)interchange the STBs configuration hardware,
- (iii)change subscriber ID,
- (iv)merge accounts.... and so on...

(h) [NB1: It is time to look and usher in DTH portability as in Telecom industry's number porting options. Assessing the efficacies of the present copy protection technologies and better DRM enforcement with measures that involve /least/minimal/ costs and that are not a burden to the subscriber or passed on to them in any way.

(i) [NB2:A Blu-Ray Player's price was sky high at launch and was out of the reach of many till it found a level...and one of the selling points for it offered better copy protection features and was stated to be more secure.....even such Blu-ray discs were eventually cracked, copied and dealt with in many ways that were meant to be proscribed in the first place.]

(j)It is the light of so many variables that a copy protection and DRM enforcement regime will have to operate after a realistic assessment is made of the ground realities before bringing in Regulations that are ideally to be followed in compliance rather than in their breach and contravention, which might happen in the situations described below in paragraph(k)

(k)Impracticable and unrealistic solutions (One such instance is discussed in paragraph (7.1)(c)above) or Regulations after being introduced hastily without a

