MPA

ASIA PACIFIC

MOTION PICTURE ASSOCIATION ASIA PACIFIC

December 9, 2019

The Motion Picture Association ("MPA") appreciates this opportunity to respond to the consultation paper released by the Telecom Regulatory Authority of India ("TRAI") on the Interoperability of Set Top Box on 11 November 2019.

MPA is a trade association representing six international producers and distributors of film and television entertainment. The MPA-represented companies are:

Walt Disney Studios Motion Pictures
Netflix Inc.
Paramount Pictures Corporation
Sony Pictures Entertainment Inc.
Universal City Studios LLC
Warner Bros. Entertainment Inc.

Our member companies produce and distribute a wide range of film and television content in India.

As the Consultation Paper rightly notes, "*Robustness of any solution regarding protection against content piracy would be key to its successful implementation and adoption by the industry*" and "*even in case of Indian Broadcasters and content providers, security of content from piracy remains primary concern. Any solution for interoperability of STB must pass the scrutiny on account of content security.*" [1] In this spirit, we propose for your kind consideration the following principles to ensure that any proposal under consideration does not inadvertently hinder the production, distribution, or security of high-value film and television content. We note that we shared these principles with TRAI in 2017 and they remain relevant.

1. The boxes must not disrupt copyright holders' rights to determine whether, how, through whom, when, where, and under what terms and conditions to disseminate their content. Additionally, any regulation must not prescribe or limit the type of contractual provisions governing the presentation or protection of content, which may be contained in the licensing agreements between content companies and distributors.

[1] Chapter 2.9, pp.24-25.

2. Anyone using the boxes to distribute copyrighted content must be in privity with the copyright holders and must abide by all license terms pertaining to that content, such as how the content is secured, presented, and commercialized; to whom the content is distributed; and how the box collects and uses data about what consumers are watching.

3. Content providers/digital platform operators must be able to test in advance and periodically audit the boxes, and to suspend the boxes' access to content if the boxes are or become insecure or otherwise out of compliance.

4. Content providers/digital platform operators must be able to determine which protection measures are employed, as well as change them in the event they become compromised or as technologies advance.

5. Set top box security must be thoroughly assessed by independent security assessment companies certified or appointed by TRAI or competent authorities. When smart cards are used, the protocol between them and the boxes must be reviewed by experts to ensure the robustness of the implementation of the boxes. When downloadable systems such as ECI are used, the security of the download system and the API interfaces between the downloaded client and the host must similarly be reviewed by experts.

6. The proposal must not inadvertently weaken content protection or chill innovation in content protection technologies. For example, MPA is concerned that the proposal to create a centralized trust authority will result in a "single point of failure". A centralized trust authority will be an attractive target for attacks, hinder effective compliance and robustness frameworks, and inhibit diversity in content protection mechanisms. For example, different distribution platforms and even different distributors using similar platforms often rely on different trust authorities. A centralized trust authority cannot accommodate such diversity. Moreover, if a centralized trust authority is compromised, then everyone's systems become compromised. Additionally, in such an event, revoking access for one compromised distributor cannot be done without revoking access for all distributors beholden to the centralized trust authority. Standardization of content protection mechanisms can similarly weaken security, as well as hinder the ability of parties to develop, experiment with, and implement diverse solutions. Such diversity itself enhances security. The proposal must therefore refrain from adopting regulations that limit the types of security solutions content providers and distributors may implement; avoiding the "single point of failure" result. Any rules and standards must also remain technologically neutral, both to accommodate different platforms and to preserve a competitive market for security solutions.

7. Similarly, the proposal must not inadvertently chill innovation in the production, distribution, and presentation of film and television content and television services. For example, content providers/digital platform operators must be able to change set top features as their content and services evolve with technology and new business models.

8. The devices must not co-mingle Internet and non-Internet content except as permitted in the content license agreements, or enable users to display both authorized and unauthorized content in search results. More broadly, the devices must not have the ability to present content in any manner that is not expressly authorized by the underlying license agreement with the distributor.

On the basis of these principles, MPA would like to comment in particular on Embedded Common Interface ("ECI"), a solution considered by TRAI to achieve interoperability. MPA is concerned that ECI does not meet the content security and technology needs of major content providers.

In 2013, MovieLabs (a consortium of major film and television studios) created a specification known as Enhanced Content Protection ("ECP"), which it updated in 2018.[2] As TRAI stated in its consultation paper, *"the ECP specification describes best practice for all premium content services, including Pay TV and live sports."* ECP includes strong content security features and the ability for our Members to forensically watermark their content distributed on home devices, set top boxes, etc. ECI falls short of the ECP requirements. In particular, ECI does not require watermarking and does not create a secure location for a watermark. Watermarked content is important: it helps our studios better address data breaches and protect content stored on computer servers.

Major Digital Rights Management ("DRM") providers are also concerned about ECI. ECI's scope goes beyond Conditional Access System ("CAS") to include DRM – but DRM does not pose an interoperability problem. Existing interoperable systems for broadcast, such as DVB Simulcrypt, may incur a small overhead in one-way broadcast streams. As noted by the expert stakeholders convened by TRAI to propose solutions for achieving interoperability, DVB Simulcrypt offers *"three key advantages (...) to operators: it provides interoperability between multiplexers, scramblers and Conditional Access Systems; it enables Conditional Access Systems to co-exist on the same network; and it prevents a CAS vendor who implements a compliant system from locking out other CAS vendors."*[3] We would add that DVB Simulcrypt does this without requiring the establishment of a third party trust authority or developing new compliance and robustness rules, as those are already well-established in the ecosystem by CAS vendors working with operators.

However, the future lies in two-way systems, and DRM has shown that multiple systems can easily co-exist: video service operators can easily stand up license servers for multiple DRMs, most Android devices use the Widevine DRM, Apple devices use FairPlay and many others, including Windows devices, use Microsoft PlayReady. Content protection has not been an impediment to interoperability in the two-way world. The experience with DRM therefore shows that two-way CAS can follow a market model for interoperability.

[2] https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

[3] https://main.trai.gov.in/sites/default/files/201605020353596014369CEAMA_0.pdf

Another major problem of ECI is that it is not accompanied by a clear and adequate compliance framework. ECI shifts compliance responsibilities (currently collaboratively administered by stakeholders and DRM providers) to a "trust authority" – making it difficult to test DRM compliance, access needed information quickly, and fix data breaches. The ECI specifications do not provide the technical compliance and robustness rules which underpin the security of the system, leaving those to a Trust Authority to define. This is a concern that video content rightsholders and major DRM providers share.

The European Telecommunications Standards Institute ("ETSI") issued ECI under a closed, industry group process, which was not subject to an open standards participation and review by all stakeholders. The specifications are currently under wider review at the ITU-T in Study Group 9. It would be premature to consider ECI until it has passed wider review and international approval and until, as we noted above, it satisfies TRAI's requirement that *"any solution for interoperability of STB must pass the scrutiny on account of content security."*

Trev Fernandes

Trevor Fernandes
VICE PRESIDENT, GOVERNMENT AFFAIRS, ASIA PACIFIC

O	(65) 6253-1033
M	(65) 9108 9959
E	trevor_fernandes@motionpictures.org