MOTION PICTURE ASSOCIATION – INTERNATIONAL

(a limited liability corporation incorporated in the United States of America)

Under license from Motion Picture Association

MPA
MOTION PICTURE ASSOCIATION
Audiovisual Entertainment
For Global Audiences

ASIA-PACIFIC OFFICE
No. 1 Magazine Road
#04-07 Central Mall
SINGAPORE 059567
TEL: (65) 6253 1033
FAX: (65) 6255 1838

25 May 2011

By email

SUBMISSION FROM THE MOTION PICTURE ASSOCIATION-INTERNATIONAL TO THE MDA CONSULTATION ON CONTENT PROTECTION SECURITY REQUIREMENTS IN SUPPORT OF THE CROSS-CARRIAGE MEASURE IN THE PAY TV MARKET

To:

Ms Eileen Ang
Head (Competition and Market Access)
Media Development Authority of Singapore
(Attention: Ruth Wong)
Email: ruth_wong@mda.gov.sg

Submitted by:

Frank Rittman
Vice President & Deputy Managing Director
Regional Policy Officer, Asia Pacific
Motion Picture Association

Krishnan Rajagopalan
Vice President, Technology
Motion Picture Association of America (MPAA)

Kindly contact us if you require further clarifications or follow-up.

Thank you

Contents

INTRODUCTION

The Motion Picture Association-International ("**MPA-I**"), a trade association representing the interests of six international producers and distributors of filmed entertainment, including television programming, submits the following comments to the industry dialogue paper entitled "Consultation on Content Protection Security Requirements in Support of the Cross Carriage Measure" ("**CP Requirements Consultation**"), issued by the Media Development Authority of Singapore ("**MDA**") on Apr 20, 2011.

On 6 May, 2010, 27 September 2010, and 18 April 2011, MPA submitted response comments to the Media Development Authority's ("MDA") Consultation Papers dated 12 March 2010, 1 September 2010, and March 23 2011 respectively, on the "Proposed Implementation Details of Remedy to Competition Issues in the Pay-TV Market" (the "First Consultation") and on "Cross-Carriage Measures in the Pay TV market.

In its first response ("First Response"), MPA highlighted the grave concern of MPA's member companies over the Singapore Government's proposed amendments to the Code of Practice for Market Conduct in the Provision of Mass Media Services ("the Code") in mandating that pay-TV operators make available channels/content which they have acquired on an exclusive basis for carriage by other nationwide subscription television service licensees not originally licensed by the content owner ("Measure").

In its second response ("Second Response"), MPA reiterated concerns regarding the sanctity of intellectual property rights and the effect the proposed Measure might have on Singapore's aspirations to be a "media hub" and intellectual property role model for the Asia Pacific.

In its third response ("Third Response"), MPA noted that in the second consultation paper issued in September 2010, the MDA confirmed its intention to proceed with the implementation of the Measure, notwithstanding concerns raised by MPA and its member companies, amongst others, that this would effectively constitute compulsory licensing, and be inconsistent with Singapore's international obligations under various intellectual property rights treaties, and focused its remarks primarily on the so-called "other implementation suggestions" referenced in paragraphs 3.13 of the third consultation paper.

In this response ("Fourth Response") to the CP Requirements Consultation, the MPA-I does not intend to repeat specific points already addressed in its three prior submissions, and instead limits its comments to identifying the many essential technical CP requirements imposed on licensees in today's marketplace prior to any consideration of the carriage of their works. The MPA-I believes it is essential that the MDA further refine these CP requirements and technical specifications prior to any proposed implementation of the Measure.

SUMMARY

Aside from our principled opposition to the Measure for the reasons already set forth in our prior submissions, the CP Requirements Consultation provides grounds for further concern from the standpoint of technical specifications. The Measure is proposed to be implemented in the vacuum of an operational infrastructure (licensing regime) that (a) develops and manages changes to the guidelines and specifications over time using a process that allows different constituents to have a reasonable voice in the process, (b) requires RQLs and their associated device manufacturers to sign appropriate licenses to gain access to the guidelines and specifications, (c) manages the certification, testing and labelling process associated with the ecosystem and (d) requires RQLs to implement a compliance monitoring and enforcement program to ensure that the security of the ecosystem is not compromised.

Successful licensing regimes in other jurisdictions (such as those operated by CableLabs, AACS, DTLA, and DCP) include all these operational elements, which are critical to the success of these standards and the wide availability of content over systems that are signatories of such licensing regimes. At present, no such independent entity capable of undertaking such functions is known to be operating in Singapore. The full implementation of the Measure should not proceed unless and until such an independent entity is so recognized and funded by the MDA with duly delegated operational responsibilities to serve as the licensing regime for all guidelines and specifications related to the Cross Carriage Measure.

Content providers impose individual security requirements on their licensees to ensure that the licensee protects content in a manner that is acceptable to the content provider and such requirements may vary across different categories of content (e.g. linear vs. VOD). Content providers have the right to negotiate new and different protection terms as their products evolve and to seek injunctive relief and damages directly against all platform operators. For example, the nature of protection used by content providers to protect their works in VOD offerings would necessarily require that they work directly with both the SQL and RQL. Overly stringent government regulation providing otherwise will hinder the continued development and evolution of these new business models. The MDA must therefore limit the scope of the Cross Carriage Measure strictly to those areas that address the content fragmentation issue that the Measure is constructed to resolve. Specifically, the MDA must exclude still-evolving business models and technologies such as advanced interactive content, 3D content and Premium Home Theatre Content from the Measure. Such business models and content require additional technical and content protection features in the operator's network and are not widely deployed today.

Additionally, the MDA must also exclude RQLs that deliver content over Relevant Platforms but use purely software-based mechanisms to protect content from the measure. Such content protection mechanisms do not protect content on par with approaches that use hardware-based schemes to protect content and are not appropriate candidates for receiving the same class of content.

This submission also contains comments about various topics referenced in the CP Requirements documents such as:

a. the approach to content protection measures
b. market-based approach for the commercial agreement between SQLs and RQLs
c. delivery of content from content providers to RQLs
d. security guidelines for the RQL headend
e. STB security and output recommendations

The view of content providers is that the MDA must clarify that these are not CP "guidelines" that "should" be observed. Our view is that these are in-fact CP requirements that device manufacturers and RQLs must meet in order to receive and process QC prior to any proposed implementation of the Measure.

STATEMENT OF INTEREST

The MPA-I represents the interests of six major international producers and distributors of theatrical films, home video products and television programming, namely:

- Paramount Pictures Corporation
- Sony Pictures Releasing International
- Twentieth Century Fox International Corporation
- Universal International Films
- Walt Disney Studios
- Warner Bros Pictures International

MPA-I member companies are primarily the content providers of filmed entertainment and television programming for more than one hundred fifty different markets around the world. Some MPA-I member companies or their affiliates also own or operate television channels carried by major pay television operators in Singapore.

The MPA-I member companies are not primarily involved in Singapore with other aspects of pay-television delivery, such as network management or the operation of platform systems. As such, our comments are necessarily limited to those issues directly confronting MPA-I member companies and do not extend to more general concerns affecting the continued growth and development of the pay-TV sector.

COMMENTS

Approach to Content Protection Measures

In section 2.2 of the CP Requirements Consultation, the MDA states that "*The first stage of the system covers the delivery of programming from the content provider to the SQL. The security requirements for this first stage are not covered by the Measure*". In section 2.3 of the CP Requirements Consultation, the MDA then states that "*Once the QC enters the RQL's headend, the*

RQL must protect the QC, based on the Content Protection Security Requirements set out in the MMCC."

On an individual basis, content providers today require security as part of their licensing agreements to ensure that the licensee securely protects content in an acceptable manner. Additionally, such requirements may also vary from one content provider to another and across different classes of content (for e.g., linear vs. VOD) for content sourced from a single content provider across content offered in different time windows.

The MPA-I accordingly recommends that the MDA allow usage rights information to be associated with individual QC and transferred from the SQL to the RQL in a secure manner, while requiring RQLs to process and distribute QC strictly in accordance with the rights specified in the usage rights information received from the SQL. Note that the usage rights information can either be carried in-line with the content or carried externally (for e.g., in the content license); it is appropriate for the any regulations to specify a minimal set of usage rights information that will be supported by the guidelines but allow for flexibility in how information about the rights are communicated to the RQL from the SQL or content provider.

Commercial Agreements between SQL and RQL

In section 2.4 of the CP Requirements Consultation, MDA proposes that the delivery process and the technical specification of QC from SQL to RQL be left to commercial negotiation.

The MPA-I agrees that if the Cross-Carriage Measure is implemented at all, it must be with this market-based approach, and further recommends the MDA clarify that the commercial agreement between the RQL and SQL may include the same security obligations on the RQL as those that the SQL has undertaken with respect to the QC based on its distribution agreement with the content provider. Specifically, the SQL – RQL commercial agreement must afford content providers third party beneficiary rights to obtain injunctive relief and liquidated damages for any breach by the RQL of the security obligations in the agreement and for any harm caused to the content provider from leaks or theft of content by the RQL or its subscribers.

Sourcing VOD files

In section 2.5 of the CP Requirements Consultation, MDA proposes that the same approach be used for both linear as well as VOD content, and states that *"Most VOD content is encoded by the CP or VOD content aggregator into a digital encoded file that can be securely delivered to the system operator over private networks or the Internet. The system operator can directly load the encoded content files onto its VOD servers and begin delivering to the subscribers' premises. This eliminates the need to encode the content from digital video tapes and conduct quality control review of the encoded files."*

Furthermore, in section 3.5.7 of the CP Requirements Consultation, MDA states that *"The SQL's application of an RQL-specific forensic watermark to track and determine potential sources of piracy of QC supplied to each RQL should be at the option and responsibility of the SQL"*

The MDA recognizes that copies of QC sent by content providers to licensees for VOD and/or linear distribution are often individualized through the use of watermarks to identify the licensee in case of theft of content either from the facility or through the distribution channel. However, the MDA fails to recognize that SQLs are not in any way involved in (and in many cases are unaware of) the generation of "source" watermarks that help content providers trace leaks from the SQL's distribution network.

This implies that RQLs must necessarily be able to receive content directly from the source (as the copy sent to the RQL may have a different "source" watermark from the copy sent to the SQL). Given that content providers will incur substantial costs in preparing customized packages for each RQL, content providers must be reimbursed (by either the SQL or the RQL) for those costs incurred as a result of the implementation of the Measure. In addition, there must be a verification mechanism whereby RQLs demonstrate to the content providers that they have secured the right to carry specific content before they receive the specific content. In other words, there needs to be a contractual arrangement between the content provider and each RQL covering these and related requirements, notwithstanding the Cross-Carriage Measure.

Additionally, the requirement that "*SQL's application of an RQL-specific watermark should be at the option of the SQL*" must be struck from the CP Requirements document.

Headend Security Requirements

Chapter 3 of the CP Requirements Consultation contains a list of requirements that an "*RQL should implement in its headend facility for creating an effective control environment, for managing physical site security, and for maintaining adequate digital network security, that will prevent theft of QC from the RQL's headend operation.*" The MDA also states that the "*network operator headend security requirements were developed based on the security best practice documents produced by MPAA".*

The MPA-I agrees that the guidelines adopted by the MDA are a good starting point for ensuring security at the RQL's headend, but would like to point out that:

a. The MPAA published guidelines are just that; guidelines. They do not in any way guarantee availability of content by any content provider to any receiving party. In fact, individual content providers may have specific requirements that differ from those outlined in the MPAA guidelines.

b. Content providers typically require their licensees (SQLs) to undertake a security audit by a trusted third party consulting firm to ensure that the licensee's facility meet their individual requirements (that are largely based on the MPAA guidelines). RQLs should likewise be required to perform audits of their facility using the same set of trusted third-party consulting firms to ensure compliance with the guidelines. Specifically, content providers and/or the SQL must have the ability to require such audit from a RQL before making QC available to such RQL.

c. Content providers should be able to require RQLs to implement additional security measures and specific technologies at the headend in order to receive specific pieces of QC, just as they do with SQLs today. As an example, RQLs may have to implement specific technologies

that allow them to securely receive content from different content providers. As a second example, some content providers also require facilities to be additionally compliant with the ISO/IEC 27001[1] Information Security Management System standard.

d. To the extent the MDA proceeds with the implementation of the Measure as a form of mandatory requirement, the suggested guidelines for headend security should likewise be elevated to the level of a requirement for any pay-TV operator in or entering the market.

Advanced Interactive and 3D Content

The MDA has clarified in the Sept 2010 consultation that *"the Measure will apply to linear and basic Video-on-Demand ("VOD") content and their supporting services. The Measure will not apply to advanced interactive content at this point of time. "*

The MPA-I understands that the MDA intends to exclude advanced interactive and 3D content from the Measure, and express support for such exclusion. The evolving nature of both the business models as well as technologies needed to support these classes of content make it very difficult to ensure seamless interoperability of such content across different distribution infrastructures and, furthermore, these classes of content do not fall into the stated scope of the Measure.

Premium Home Theatre Business Model

In section 3.5.8 of the CP Requirements Consultation, the MDA acknowledges that *"there may be cases where the SQL has agreed with a CP to apply a transactional forensic watermark to track and determine potential sources of piracy of each instance of QC accessed by each SQL subscriber*", and goes on to state that "In *the case where an SQL has agreed and is complying with such a transactional watermarking obligation for QC (for example, transactional watermarking applied in the subscriber's set-top box during viewing of an early-window, high definition VOD movie), then the RQL will also be obligated to apply transactional forensic watermarking for such QC accessed by each of its subscribers."*

Distribution of Early-Window, Premium High Definition VOD motion pictures or Premium Home Theatre ("PHT") is a very new business model that is the subject of experimentation by some content providers in limited territories; it is not yet a fully implemented or widely deployed form of distribution. A PHT offering would make available to subscribers HD motion pictures that have been recently released in theatres, but have not yet been made available to the public on any of the traditional home video distribution channels such as DVDs or BDs or electronic home video. The security requirements for such content tend to be very complex and specific to individual content providers, and include measures such as the authorization of only specific protected digital outputs for display, the approval of specific forensic watermarking technologies and approaches (head-end vs. STB) that take the operator's network configuration into account, an operational process to identify illegal copies of content on the Internet and track offenders based on the forensic mark.

[1] http://en.wikipedia.org/wiki/ISO/IEC_27001

Given the additional security requirements, the experimental nature, and the business complexities involved in launching a PHT offering, and the lack of connection between PHT and the problem of content fragmentation that the Measure addresses, content providers feel strongly that the MDA must also exclude Early-Window HD VOD content from the requirements of the Cross-Carriage Measure at this time. At such time that the PHT business model matures and is widely deployed in Singapore (or comparative markets in the Asia/Pacific region), this question may perhaps be revisited at that time along with appropriate input from the content providers who have pioneered such distribution model.

Content Protection Delivery System Security Requirements

In section 4.2 of the CP Requirements Consultation, the MDA states that "*In the Proposed Guidelines, the term CPDS will apply to both RSPs using CAS systems for protecting and controlling access to high-value pay TV content and also to RSPs using DRM technologies. The same requirements apply to both types of system*".

The MPA-I respectfully comments that a majority of content providers around the globe today differentiate between CAS systems for protecting Pay TV content and RSPs using DRM technologies. CA systems that provide hardware-based security mechanisms that access content through dedicated STBs in the subscriber's home provide much better protection to content than DRM technologies that allow subscribers to access content from their PCs or other "open" devices, and business models today take these different security capabilities into account. Due to such differing security environments, among other factors, feature-length motion pictures and new television series are typically offered on Pay TV networks with CA systems on a PPV or VOD basis well ahead of such content being made available to RSPs who use DRM technologies to deliver content to a variety of "open" end user devices such as PCs, tablets and smartphones.[2]

We welcome the clarification from the MDA that Relevant Platforms that are candidate RQLs for this measure as those that deliver QC over:

(i) a hybrid fibre-coaxial network; or
(ii) a managed network using Asymmetric Digital Subscriber Line technology; or
(iii) a managed network over optical fibre - (also known as Next Generation Nationwide Broadband Network, "NGNBN"),

and support the exclusion of services that deliver content over public IP networks from this measure.

In addition to limiting the measure to those RQLs that deliver QC over Relevant Platforms, the Cross Carriage Measure must also distinguish between operators who use CA systems and those who use DRM technologies, and should limit the cross carriage obligation to those RQLs who use hardware-based CA or DRM systems to make QC available to their subscribers using dedicated STBs. Specifically, the MDA must exclude RQLs that deliver content using purely-software based protection schemes (DRMs), even if they do so over a Relevant Platform, from the measure.

[2] For purposes of this discussion, DRM systems that are deployed on closed/dedicated STBs and use a hardware root-of-trust to securely protect keys are considered on par with CA systems.

STB Security

STB Outputs

Commercially acceptable practice would be to require all analog outputs to carry CGMS-A and Macrovision APS analog copy protection signals as specified by IEC 62375, ETSI EN 300 294, CEA 608 and 805, and other standards, as applicable. A sunset date for all analog outputs and mandate that STBs manufactured after the specified sunset date no longer carry analog outputs is advisable, as other content protection standards are either actively considering or have already implemented. AACS (Advanced Access Content System that protects Blu-Ray discs), for example, has tiered analog sunset dates with the final analog sunset that prohibits the manufacture or sale of AACS device with analog outputs after December 31, 2013.

With respect to the circumstances under which DQC can be output over High Definition Analogue Outputs (Section 5.5.8), the MPA-I notes that high definition analogue outputs are rarely, if at all, available through pay TV systems (or other distribution schemes such as physical media and OTT delivery), and therefore urges that the following rules be adopted in lieu of those outlined in the CP Requirements Consultation:

a. DQC should not be output over any analogue output if the content is marked with a Digital Only Token (DOT). In addition, if the DOT is asserted, content can only be output on protected digital outputs which do not further output on High Definition or Standard Definition Analog Outputs.

b. If DOT is not asserted in the content, DQC should be output over 1080i60/720p60/1080i50/720p50 analogue component video output in an image-constrained format unless the SQL has approval from the CP to output the QC in HD format over analogue outputs

Finally, a mechanism[3] must be included to add protected digital interfaces to the STB requirements over time. Any digital outputs added to the STB guidelines, however, should always be protected with the appropriate link protection scheme (such as HDCP or DTCP). A number of protected digital interfaces (such as HDBaseT[4] and WirelessHD[5]) provide enhanced options for connectivity between end devices in the consumer home and should be considered.

---

[3] CableLabs operates a change management process for approval of new outputs as outlined in http://www.cablelabs.com/opencable/udcp/downloads/DigitalOutputs.pdf

[4] http:// *www.hdbaset.org*

[5] http://www.wirelesshd.org

Ability to Support Rich Usage Rights

Any security solution proposed for the STB guidelines must support the expression of a wide range of usage state information for any particular piece of content (which the content owner can select, e.g. through use of a CAS technology), support the carriage of such information in the broadcast stream, and require adherence at the STB to comply with the authorized usage rules. This will encourage innovation and multiple business models for a wide range of content.

The following usage rules for the STB guidelines should be applied on a content by content basis:

i. Ability to control propagation (view, move, copy) of the content across devices in the subscriber's domain[6];

ii. Ability to limit re-distribution of content;

iii. Ability to selectively enable outputs (with associated content protection schemes) through which the content can be viewed, moved or copied onto other devices (this should include the ability to limit the output of content only through a specific protected digital interface); and

iv. Ability to require devices to scale down the resolution of the content when passed through analog outputs.

The DVB CPCM Usage State Information[7] specification, which provides a comprehensive set of usage rights that can be expressed with respect to DRM-protected content, provides information that can be used to enhance any proposed implementation of the Measure over time; support for such usage rights information will allow new and innovative business models to be supported on the Relevant Platforms.

Application Frameworks and Open Access to Internet on STBs

Content providers today work individually with Pay TV operators to control access to general content from the Internet including infringing content from authorized set top boxes supported by the operator. The MDA CP requirements in support of the Measure must limit access to infringing content from STBs that are used to consume QC.

---

[6] Most new CA and DRM technologies use the concept of a "domain" as an approximation of a "household". DVB CPCM defines a domain as *"A distinguishable set of compliant devices, which are owned, rented or otherwise controlled by members of a single household. A household is considered to be the social unit consisting of all individuals who live together, as occupants of the same domicile. This makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household."* A number of new content services (such as Apple iTunes, and UltraViolet) support this concept and are good references for domain configuration parameters such as the number of devices, joining criteria, etc.

[7] DVB BlueBook A094r4-3 available at http://www.dvb.org/technology/standards/. (Part 3 of Blue Book A094).

Compliance and Robustness rules for devices that access QC should contain additional obligations for devices that allow users to install applications. In such cases,

- RQL must implement application certification procedures (including procedures to certify new versions of applications and review already-approved versions of applications in certain events) to ensure that applications do not provide access to infringing content or pose security threats to the device environment before such applications are made available as certified applications or widgets that can be enabled on licensed devices by end users;

- Licensed devices must ensure that they can execute only certified applications;

- MDA guidelines must specify compliance and robustness rules that govern the ongoing operation of applications and devices so that appropriate enforcement actions may be taken against any devices and applications that compromise the security of the licensed device or provide access to infringing content online once enabled; and

- RQL must implement a compliance monitoring and enforcement program to immediately disable any applications and devices that do not meet the compliance and robustness rules.

In addition, licensed devices that allow access to the open Internet through a browser mechanism:

- Shall not allow access to locations on a URL Blacklist using the browser or any other function on the licensed device. Processes for maintaining entries in the URL Blacklist and secure interfaces to retrieve the URL Blacklist will be defined either by the licensing regime for this Measure or by content providers.
- Shall check for updates to the URL Blacklist on every boot.
- If there is no IP connectivity at boot time, licensed devices shall check the server for URL Blacklist updates as soon as IP connectivity is possible.

Audio Watermark Screening and Enforcement Requirements

The licensing regime associated with the Measure must include obligations on the Licensed devices to include an Audio Watermark Detector and screen for the presence of the "No Home Use" and "Trusted Source" Cinavia™ Audio Watermarks in all content that is decoded and played back on the licensed device.

- The Audio Watermark Detector shall perform screening pursuant to the requirements set forth in the Cinavia Specifications. For the avoidance of doubt, the Audio Watermark Detector must screen for the "No Home Use" and "Trusted Source" states irrespective of whether such content is encrypted or whether such content carries the AACS flag.
- The Audio Watermark Detector's screening process should be activated every time content is played back on the licensed device. The screening process must be activated in continuous mode as opposed to the intermittent mode.
- On detection of a Cinavia watermark, the licensed device must take action to prevent playback of content consistent with Cinavia's guidelines for such detection.

Copy Control Watermark Non-Interference

In Section 5.5.12 of the CP Requirements Consultation, MDA states that *"If the RQL complies with the foregoing provisions...and RQL should be able to incorporate legitimate features (e.g. recompression, image overlays, video mixing, etc.)"*. MPA-I instead opines that RQLs, like SQLs, **must** (emphasis added) obtain permission from content providers before incorporating such features as they could adversely affect the video quality, the context of the program content, or in certain cases the intended branded experience.

Robustness rules for design and manufacture of set-top box receivers

In section 5.6.9 of the CP Requirements Consultation, MDA lists a minimal set of techniques to make robust the functions and protections outlined in the document. The requirements listed in that section must be strengthened considerably before they can be considered effective protections against hacks. For example, section (e)(i) identifies a very low standard by specifying that device manufacturers must implement protections in a manner that *"cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that is widely available..."*. We note that a majority of the hackers who attack content protection schemes have access to sophisticated tools and techniques; protecting against "general purpose tools" is not sufficient to protect against hacks from even casual hackers in the current environment and that the current requirement does not ensure that devices will be sufficiently robust against attacks.

Implementation and Review of Proposed Guidelines

In section 6.1 of the CP Requirements Consultation, MDA proposes to implement the Proposed Guidelines through a certification process, and seeks comments on whether the process should allow for self-certification by the RQL or joint-certification by the RQL and the SQL, or require independent certification.

The MPA-I notes that the proposed guidelines are based on the Compliance and Robustness Rules defined in the United States cable industry's CableLabs Tru2way Host Device License Agreement, and believe that these are an appropriate starting point for any proposed implementation of the Measure. We however note that content providers in the United States rely heavily on the licensing regime operated by CableLabs to enforce the terms of the license[8]. The licensing regime operated by CableLabs is in fact more important than the technical specifications related to the DFAST and Tru2Waytechnologies, as it ensures that the ecosystem operates in accordance with the outlined guidelines.

The MPA-I believes that self-certification or joint certification by the SQL and RQL are not effective mechanisms to protect the security of the distribution ecosystem, and strongly urges the MDA to

[8] See http://www.cablelabs.com/opencable/downloads/tru2way_agreement.pdf for the Tru2Way license agreement that device manufacturers must sign in order to manufacture Tru2Way devices. The unidirectional interface is similarly implemented through a host of licenses available at http://www.cablelabs.com/opencable/udcp/ and maintained by the CableLabs licensing regime.

instead appoint an independent authority or market entity to manage the process[9]. The selected licensing and certification authority must:

a. define a comprehensive certification program that is approved by content providers before the standards and specifications are finalized and made available to adopters.

b. require stringent security audits before certifying STBs that are capable of receiving QC. The audits should include, at a minimum, a test to ensure that the security requirements in each device have been robustly implemented in accordance with the Robustness Rules (as described in the Guidelines) and a check to ensure that each test device materially conforms with the Compliance Rules (as described in the Guidelines).

c. require operators and device manufacturers to sign appropriate license agreements pursuant to which such participants obtain: (a) access to relevant technical specifications and guidelines; (c) access to security infrastructure as appropriate; and (d) a license to use an appropriate label on its devices. Only participants who sign such a license should have access to the foregoing elements; moreover, the license itself should require full compliance with its requirements. The license should only allow participants who are in full compliance with the requirements to obtain a license in the first instance and only allow such fully compliant licensees to gain access to any of the foregoing documents and privileges. Furthermore, the license agreement should contain the standard terms that are usually found in content protection technology licenses, including, without limitation, the following:
    1. Third party beneficiary rights to obtain injunctive relief and liquidated damages for breach of the license agreement;
    2. Change management rights by content providers
        i. An established, flexible procedure to easily react to changing market needs (such as approving new outputs, changing specifications, addressing stolen keys, etc), along with an escalation/arbitration process overseen by the MDA to resolve disputes.
    3. Revocation and renewal procedures that must be implemented by RQLs;
    4. Compliance Rules. The Compliance Rules common in the industry typically impose on the licensee the following requirements, among others:
        a. Content usage rules;
        b. Approved outputs, with appropriate content protection signalling; and
        c. Approved DRMs and CA systems that can be used by RQLs
    5. Robustness Rules. The Robustness Rules common in the industry typically impose on the licensee an obligation to robustly implement the security features of the device to prevent tampering.

[9] CableLabs is the independent authority that maintains the Tru2Way and DFAST licenses and serves as the licensing and operational trust regime for the ecosystem.

d. ensure that RQLs monitor the marketplace for compromised or unlicensed devices and take immediate action against any breach in security through revocation and renewal, court action for injunctive relief and/or damages, and/or by termination of the license.

The CableLabs regime in the United States (upon which the MDA has ostensibly modelled its proposed guidelines) has been effective and successful largely due to its licensing regime which supports all the elements referred to above[10]. Such a licensing regime is also a standard and essential component of many other successful content protection specifications (including but not limited to those managed by DVD CCA, AACS, DTLA, CI Plus, and DCP). A licensing regime such as the one described above will provide an effective contractual relationship between the RQL and content providers; RQLs will be signatories to the license which will provide third party beneficiary rights to content providers in the case of material breaches of the license by the RQL.

For all the reasons outlined above, the MDA must fund and recognize an independent certification and licensing regime to oversee the maintenance and rollout of the Measure's implementation.

SingTel and StarHub as RQLs

The MDA has stated that it "*understands that SingNet Pte Ltd ("mio TV") and StarHub Cable Vision Limited ("SCV"), the two nationwide subscription television service licensees likely to be designated RQLs have already deployed content protection systems and anti-piracy measures which MDA understands are acceptable to international content providers.*"

The MPA-I again notes that its members individually assess the content protection systems and anti-piracy measures provided by potential licensees, and that, in any case, both SingTel's mioTV as well as StarHub Cable Vision Ltd must meet both the CP requirements set forth in the MDA guidelines as well as individual content provider requirements for secure receipt and processing of the QC before being approved as RQLs that can receive QC from that content provider.

[10] See http://www.cablelabs.com/certqual/ for additional details about the CableLabs certification process for Tru2Way devices; http://www.cablelabs.com/opencable/documents/ for the CableLabs licensing agreements for device manufacturers and adopters; http://www.cablelabs.com/opencable/downloads/oc_spec_change_process.pdf for the change management process (we note that the MPA has an MoU with CableLabs that allows it to collaborate with CableLabs on any changes made to the standards and licenses, and separately has the ability to independently approve additional outputs to the CableLabs DFAST license using a four studio approval process).

CONCLUSION

The MPA-I and the producers and distributors it represents continue to have grave concerns with the proposed cross-carriage regime, as set forth in all the Media Development Authority's (MDA) consultation documents, including its most recent version issued on 1 September 2010 entitled "Consultation on the MDA's Preliminary Policy Positions." These concerns include the view that MDA's approach, as framed in its consultation papers to date, violates Singapore's obligations under the World Trade Organization (WTO) and World Intellectual Property Organization (WIPO) agreements as well as the US-Singapore Free Trade Agreement. Moreover, we believe the MDA's stated approach for implementation will disrupt materially the means by which content providers and channels are compensated in the market.

This submission is primarily focused on the CP requirements and technical specifications considered by content providers as essential requirements for the secure carriage of their works by any proposed licensee. It is likewise essential that any proposed implementation of the Measure also and first take these views and comments into consideration. Because we believe it is unlikely that the perceived concerns can be adequately addressed before the proposed June 30, 2011 implementation date, we again urge a further postponement (or outright abandonment) of the Measure in order to better ensure the continued development and evolution of Singapore's pay-TV market.

Respectfully,

Frank S. Rittman