

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Video Device Competition	)	MB Docket No. 10-91
	)	
Implementation of Section 304 of the Telecommunications Act of 1996	)	
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	PP Docket No. 00-67
	)	

**REPLY OF DIGITAL TRANSMISSION LICENSING ADMINISTRATOR LLC  
TO "ALLVID" NOTICE OF INQUIRY**

Date: August 12, 2010

Michael B. Ayers  
President  
Digital Transmission Licensing  
Administrator, LLC  
949.461.4714  
Michael.Ayers@tais.toshiba.com

Seth D. Greenstein  
Constantine Cannon LLP  
1301 K Street NW, Suite 1050 East  
Washington, D.C. 20005  
202.204.3514  
sgreenstein@constantinecannon.com

## TABLE OF CONTENTS

TABLE OF CONTENTS.....	ii
SUMMARY .....	iii
I.    DTCP Effectuates Content Protection Throughout the Home and Personal Network through Technological and Contractual Obligations. ....	2
A.    DTCP Protects Content that Arrives in the Home in Protected Form. ....	3
B.    DTCP Does Not, and Should Not, Protect All Information from an AllVid Adapter.....	5
II.   DTCP has Ample Flexibility to Support MVPD and Content Owner Business Models.....	7
A.    DTCP Supports Consumer Rights of Home and Personal Networking and Recording.....	7
B.    DTCP Flexibly Supports Additional MVPD and Content Owner Business Models.....	11
1.    DTCP Can Support Video Rental Models.....	11
2.    DTCP Can Support New Services, such as those Defined in the MPAA Waiver Order.....	13
3.    DTCP Can be Adapted and Expanded to Support Additional Business Models. ....	13
C.    DTCP Can Support Required DRM Systems for Advanced Services.....	14
III.  DTCP Provides Robust Protection for MVPD-Delivered Content.....	17
CONCLUSION.....	19

## **SUMMARY**

The Digital Transmission Licensing Administrator LLC (“DTLA”) concurs with many commenters that the content protection technology licensed by DTLA, particularly DTCP-IP (Digital Transmission Content Protection for Internet Protocol), can play a positive role in integrating into the home network MVPD content delivered over an AllVid adapter. In responding to several comments, DTLA addresses in this Reply certain misconceptions about the nature and operation of DTCP.

First, DTCP-IP ensures end-to-end protection for content that the consumer receives in a protected form (such as conditional access MVPD transmissions or encrypted optical disc). The DTCP technology re-protects that content as it traverses between devices connected to the home network. The DTCP license obligations assure that devices that record DTCP-protected content will follow the Encoding Rules of the Commission and DTLA, and that devices that retransmit content received protected with DTCP will continue to transmit that content only over outputs that offer protections no less stringent than DTCP. Because this chain of protection can effectively be required by license, and by adoption of the DLNA guidelines, no regulatory mandate is needed.

Second, the Commission does not need to provide that DTCP should protect all content transmitted via an AllVid adapter. Under the Encoding Rules, content transmitted over terrestrial broadcast channels is not required to be protected on the home network. Unidirectional and bidirectional communications to and through the AllVid adapter, such as those which enable channel selection and other operational functions, can be delivered robustly in the clear, and need not be encrypted by DTCP, across the home network.

Third, DTCP provides consumers, content owners and manufacturers with a high degree of flexibility. DTCP allows content to be streamed throughout the home network, but deters retransmission beyond the home and personal network. DTCP permits consumers always to record subscription content, and allows copies to be moved from temporary storage (such as a DVR) to another temporary storage medium or to a permanent medium (such as a recordable optical disc). DTCP already supports business models such as rental for defined periods, or advance home access to theatrical motion pictures pursuant to the recent selectable output control waiver order. DTLA remains open and willing to adapt DTCP so as to assist content owners and MVPDs to facilitate additional and future business models.

Fourth, DTCP provides robust protection using well-tested government and industry-standard technologies and techniques. DTCP interoperates with numerous current content protection technologies, including DRM systems. DTLA is pleased to work with proponents of other existing and future technologies to expand the list of compatible technologies.

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Video Device Competition	)	MB Docket No. 10-91
	)	
Implementation of Section 304 of the Telecommunications Act of 1996	)	
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	PP Docket No. 00-67

**REPLY OF DIGITAL TRANSMISSION LICENSING ADMINISTRATOR LLC  
TO “ALLVID” NOTICE OF INQUIRY**

In its Comments to the Commission’s Notice of Inquiry in the above-captioned proceedings,<sup>1</sup> the Digital Transmission Licensing Administrator LLC (“DTLA”) explained how its digital transmission content protection technology, known as “DTCP,” could support the AllVid approach by providing effective protection for certain audiovisual content sent across the home and personal network. In brief:

- The Digital Living Network Alliance (“DLNA”) assembled a suite of protocols used to transmit content and data between the AllVid adapter and a home network (the “DLNA guidelines”). DTCP for Internet Protocol (“DTCP-IP”) is referenced in the DLNA guidelines as a method to protect certain audiovisual content.

---

<sup>1</sup> Comments of Digital Transmission Licensing Administrator, LLC (July 13, 2010) (“DTLA Comments”).

- DTCP-IP ensures seamless interoperability and end-to-end protection for conditional access-protected content by handing off protected content only to devices that will perpetuate the usage rules.
- DTCP can promote new business models such as those identified in the Commission’s grant of the waiver request to promote early-window MVPD delivery of theatrical movies,<sup>2</sup> and defined movie rental periods.<sup>3</sup>
- DTCP can carry information to interoperable DRM systems so as to enable additional business models and downstream protections.

Numerous comments agreed DTCP could play a constructive role in assuring that content remains protected in accordance with the Commission’s Encoding Rules.<sup>4</sup>

However, several comments raised questions concerning how DTCP could accommodate the AllVid concept; and others demonstrated misunderstandings as to the nature and operation of DTCP, the protections offered by the technology and its licensing structure, and its flexibility to address future needs. With apologies for any repetition, DTLA clarifies below how DTCP addresses the concerns raised by these comments.

**I. DTCP Effectuates Content Protection Throughout the Home and Personal Network through Technological and Contractual Obligations.**

DTCP is a “link” technological protection method. Functionally, DTCP establishes a secure authenticated channel between all devices on a network that

---

<sup>2</sup> *In the Matter of Motion Picture Ass’n of America, Petition for Expedited Special Relief; Petition for Waiver of the Commission’s Prohibition on the Use of Selectable Output Control*, (47 C.F.R. § 76.1903), CSR-7947-Z, MB Docket No. 08-82, Memorandum Opinion and Order (rel. May 7, 2010). See Comments of DTLA in that proceeding (July 21, 2008).

<sup>3</sup> Digital Transmission Content Protection Specification Volume 1 v.1.6 at 67 (Mar. 19, 2010), [http://dtcp.com/documents/dtcp/Info\\_20100319\\_DTCP\\_V1\\_1p6.pdf](http://dtcp.com/documents/dtcp/Info_20100319_DTCP_V1_1p6.pdf) (hereinafter “DTCP Specification”).

<sup>4</sup> 47 C.F.R. § 76.1904. DTLA notes that the Encoding Rules established in the DTLA agreements dovetail with the Commission’s Encoding Rules. References to “Encoding Rules” hereinafter therefore refer to both the Commission and DTLA rules.

implement DTCP, and transmits content in encrypted form only to those devices. DTCP also provides a crucial link in a chain of contractual obligations that ensure end-to-end protection for audiovisual content, from its initial source throughout the network:

- Content owner licenses to networks and MVPDs require content to be encoded with DTCP, in accordance with the Commission's Encoding Rules.
- Set-top boxes licensed to decrypt MVPD conditional access methods are required by that license to output protected content using only protected connections, including DTCP.<sup>5</sup>
- DTCP licenses require that devices permitted to receive DTCP-protected content must follow specific storage and output protection rules even when using technologies other than DTCP.

This combination of strong technological methods plus legal obligations to only permit content to flow to devices that are contractually obliged to incorporate and observe the rules of such technologies, provides end-to-end protection for content from the MVPD to devices on the home network.

**A. DTCP Protects Content that Arrives in the Home in Protected Form.**

As noted in DTLA's Comments at 2, certain audiovisual content is delivered to consumers only in protected formats. As a few examples, MVPDs encrypt transmitted content and deploy conditional access systems, so that consumers access only those channels to which they have subscribed and that content for which they separately have paid (such as pay-per-view or video-on-demand); Blu-ray discs are encrypted using AACS; and DVDs are scrambled using CSS. These technological measures are intended

---

<sup>5</sup> See, e.g., <tru2way> Host Device License Agreement, Exhibit C Compliance Rules § 2.4 (July 1, 2010), [http://www.cablelabs.com/opencable/downloads/tru2way\\_agreement.pdf](http://www.cablelabs.com/opencable/downloads/tru2way_agreement.pdf); Amended and Restated Nonexclusive CableCARD-Host Interface License Agreement, Exhibit C "Compliance Rules" § 2.4.1, at 37, <http://www.cablelabs.com/opencable/downloads/CHILA.pdf>.

initially to limit access to the protected content only to products that are authorized to descramble or decrypt those technologies. However, content owners have observed that protecting content when delivered to the consumer would have limited value if the content could then be digitally copied in the clear and redistributed, or retransmitted outside the home network such as over the internet, without any restriction. Therefore, the licenses to decrypt or descramble the content pursuant to these initial access control measures further require that receiving devices “downstream” must continue to protect that content against unauthorized copying or unauthorized retransmission outside the home and personal network.

DTCP is intended as a measure to re-protect such audio and audiovisual content in transit between devices connected on a home or personal network. The DTLA agreements permit DTCP to be encoded only with respect to “Commercial Entertainment Content,” which is defined as “works, including audio, video, text and/or graphics, that are (a) not created by the user of the Licensed Product; (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual or a small, private group; and (c) received by a Commercially-Adopted Access Control Method ... .”<sup>6</sup>

---

<sup>6</sup> See Content Participant Agreement: Audiovisual Version (“Content Participant Agreement”), at 2-3 (definitions, including Commercial Audiovisual Content”), § 2 at 8-9 (license and scope of use clauses), § 5 (Encoding Rules) at 19-24, [http://dtcp.com/documents/licensing/DTCP\\_Content\\_Participant.pdf](http://dtcp.com/documents/licensing/DTCP_Content_Participant.pdf); Digital Transmission Protection License Agreement (“Adopter Agreement”), § 5.5 at 10 (scope of use clause) and Exhibit B Compliance Rules § 2.8 at B-3 (definition), [http://dtcp.com/documents/licensing/DTLA\\_Adopter\\_Agreement.pdf](http://dtcp.com/documents/licensing/DTLA_Adopter_Agreement.pdf). The definition also permits protection of broadcast content pursuant to a governmental legislative or regulatory mandate. In that connection, DTLA anticipates that the definition will be

DTCP is not intended to protect information that should otherwise be transmitted between devices in the clear. This includes terrestrial broadcast television programming which, under the Encoding Rules, cannot be encrypted, and user-generated content. Thus, the comment from Echostar and Dish Networks, that DTCP should be applied “only to such content as was encrypted in its original transmission,”<sup>7</sup> is thoroughly consistent with the purpose and operation of DTCP under its existing license agreements.<sup>8</sup>

**B. DTCP Does Not, and Should Not, Protect All Information from an AllVid Adapter.**

One commenter suggested that DTCP was somehow limited because it did not include means to convey video commands among devices on the home network.<sup>9</sup> This

---

amended to permit DTCP encoding (using Copy One Generation and EPN encoding) of certain content made available over the United Kingdom High Definition (HD) Digital Terrestrial (DTT) system, pursuant to governmental regulatory approval from Ofcom. See “Statement on content management on the HD Freeview platform” (June 14, 2010), [http://stakeholders.ofcom.org.uk/binaries/consultations/content\\_mngt/statement/statement.pdf](http://stakeholders.ofcom.org.uk/binaries/consultations/content_mngt/statement/statement.pdf).

<sup>7</sup> Joint Comments of Dish Network L.L.C. and Echostar Technologies L.L.C. at 13.

<sup>8</sup> The comments of Syphermedia Int’l suggest that DTCP is intended to protect only compressed in-the-clear content. Comments of Syphermedia Int’l, Inc. at 4. DTLA is uncertain as to the meaning of this comment, but offers the following clarifications. First, DTCP re-protects content delivered to the consumer in a protected form (generally encrypted, but in specific cases through a system with an appropriate enforcement mechanism such as the UK HD DTT system cited in n.6, *supra*), so content delivered to the consumer in-the-clear would not be protected by DTCP. Second, DTCP can be used to re-protect such content both in compressed and uncompressed forms. Third, the Adopter Agreement does impose a requirement that the video portion of Decrypted DT Data shall not be present on any user-accessible buses of a sink device in analog or unencrypted compressed form. Adopter Agreement, Exhibit C Robustness Rules § 2 at C-1. This requirement was one of several changes added to the Robustness Rules in 2005 that came into effect at the end of 2006; and DTLA can update its rules if necessary with additional robustness protections that are technologically and commercially feasible. Thus, contrary to the comments of Syphermedia, content protected with DTCP is not unprotected or in-the-clear in compressed digital form in a DTCP Licensed Product.

<sup>9</sup> Comments of MPAA at 5-6.

limitation misapprehends the role of DTCP in the home network. As DTLA observed in its Comments, functions such as device discovery, channel selection, remote signaling, networking, and upstream communications are adequately addressed by the DLNA and UPnP standards developed cooperatively by representatives of all affected industry segments.<sup>10</sup> DTCP complements the role of those DLNA protocols by protecting certain content as it traverses the network using those DLNA guideline protocols.

DTCP need not be applied to data associated with television operations in the home, such as channel selection or EPG data. Such data may enable the viewing of protected content, but DTLA knows of no reason why this operational data itself would need to be encrypted when exchanged on a home network between networked devices and the AllVid adapter. Such protection could add unnecessary complexity to a host of devices, including remote controls, without any concomitant security benefit for the content to be displayed or recorded. To the extent such channel selection information is transmitted outside the home network (*i.e.*, between the AllVid adapter and the MVPD), that data would be under the control and protection of the MVPD's security methods, not DTCP. Moreover, channel selection and EPG data also pertain to terrestrial broadcast content that cannot be protected using DTCP pursuant to the Encoding Rules, as well as to content that the content owner may not wish to protect. No purpose would be served by protecting channel selection or EPG data relating to content that itself is not to be protected.<sup>11</sup>

---

<sup>10</sup> DTLA Comments at 8.

<sup>11</sup> The comments of one MVPD appear to assume that the Commission intended DTCP to be used upstream from the AllVid adapter to the head-end or server. *See* Comments of Time Warner Cable at 17 (erroneously asserting that DTCP is incompatible

For such reasons, DTLA does not believe it is either necessary or appropriate for DTCP to protect every bit that emanates from, or is transmitted to, the AllVid adapter. That DTCP only encrypts data that *should* be protected within the home is a strength, and is in no way a limitation, of the DTCP technology and its licensing terms.

## **II. DTCP has Ample Flexibility to Support MVPD and Content Owner Business Models.**

Part of the functionality provided by a “link” technology is to convey rules set by the content owner downstream to other technologies that may need to act upon them. As many commenters observed, DTCP conveys the information required to implement downstream the Encoding Rules governing recording and copying of protected MVPD-delivered content. Nevertheless, certain comments appeared to misapprehend not only some of the existing capabilities of DTCP but also its flexibility to respond to future business requirements. DTLA addresses these comments below.

### **A. DTCP Supports Consumer Rights of Home and Personal Networking and Recording.**

The most basic functions facilitated by DTCP are home networking, and personal time-shifting and recording of protected content in accordance with the Encoding Rules.<sup>12</sup> With respect to home networking, as noted above, content protected with DTCP

---

with certain video systems, including IPTV). As noted in DTLA’s Comments, and as described above, DTCP does not address protection upstream from an AllVid adapter, which is the responsibility of an MVPD’s conditional access technology. DTCP is designed for use on a home network, and in that capacity clearly can protect content delivered via a variety of methods, including IPTV, as output to the home network.

<sup>12</sup> The Media Bureau recently observed that the Commission’s 2003 rules required use of the IEEE 1394 interface (with DTCP protection) on cable-supplied set-top boxes so as to promote home networking and consumer recording capabilities. *See*

can be sent across the home network to all DTCP-enabled devices in any room of the house.<sup>13</sup> That content can be output from those devices using DTCP or other approved output protection technologies (*e.g.*, HDCP or Windows Media DRM 10 and above).

With respect to home recording, DTLA negotiated its Encoding Rules with content owners and MVPDs so as to preserve consumers' reasonable and customary rights to record audiovisual content for their personal use. MVPD transmissions encoded with DTCP will be output from the DTCP "source" function with information concerning three copy control states: Copy Freely (not to be protected with DTCP)<sup>14</sup>; Copy One Generation; and, Copy Never (for pay-per-view or video-on-demand).<sup>15</sup> The Adopter Agreement requires the "sink" function of a DTCP Licensed Product receiving DTCP-protected content to respond to that encoding by permitting the copying of content marked Copy One Generation (and re-marking that copy as "No More Copies"); and refusing to permit copying of content marked Copy Never. The Adopter Agreement

---

*In the Matter of Intel Corporation, Motorola, Inc., TiVo, Inc. Requests for Waiver of Section 76.640(b)(4)(ii) of the Commission's Rules, CSR-8229-Z, CSR-8251-Z, CSR-8252-Z, Memorandum Opinion and Order ¶ 2 (June 18, 2010).*

<sup>13</sup> Pursuant to the DTCP Specification, a single content stream can be simultaneously shared with up to 34 DTCP-enabled sink devices, which should be more than adequate to accommodate the needs of the most demanding home network applications. DTCP Specification, Appendix C at 70.

<sup>14</sup> DTCP protection cannot be applied to the transmission of terrestrial broadcast content in the United States or to other content marked "Copy Freely." Adopter Agreement, Exhibit B Compliance Rules § 2.14 at B-4.

<sup>15</sup> A fourth state, "No More Copies," applies to copies made from Copy One Generation content, but such content would not be transmitted by an MVPD. *See* Adopter Agreement, Exhibit B Compliance Rules § 2.27 at B-5. A fifth state, Encryption Plus Non-assertion of numerical copy controls ("EPN") permits the making of encrypted copies without restriction, but restricts electronic redistribution of the copied content outside the home or personal network.

specifies technologies that can be used to make those permitted copies, including nine commonly used consumer recording methods.<sup>16</sup> The Adopter Agreement also permits recording of protected content using “bound” copy protection methods of a manufacturer’s choosing, without DTLA approval, so long as the recorded content is encrypted, no further usable copies can be made from it, and it can only be played on the device that made the recording.<sup>17</sup>

DTCP also facilitates the transfer of a copy made on one device to another device. DTCP long has supported a “Move” function whereby copies made on one temporary storage medium can be transferred to other devices (such as another DVR, a laptop, or a portable device) or to a more permanent recording media (such as a recordable Blu-ray disc or DVD).<sup>18</sup> DTCP’s “Move” capability gives consumers substantial flexibility in where and how to store and playback recordings they make from MVPD services. There is no prohibition on transcoding that copy to make it viewable on devices that use other media formats.

---

<sup>16</sup> See DTLA, Approvals for Persistent Storage and Digital Output Reprotection, Technology, <http://dtcp.com/approvedtechnologies.aspx>. DTLA approves these technologies under criteria that ensure that these technologies will provide technical and legal protections no less stringent than those provided by DTCP. See *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, MB Docket 04-64, Order ¶ 12 at 8 & n.48 (Aug. 12, 2004). DTLA has not refused a request for approval from any technology proponent, and has not charged any technology proponent any fee to enable such interoperability.

<sup>17</sup> See Adopter Agreement, Exhibit B Audiovisual, Part 1: Compliance Rules for Sink Functions § 2.2.1.2 at B-8, [http://dtcp.com/documents/licensing/DTLA\\_Adopter\\_Agreement.pdf](http://dtcp.com/documents/licensing/DTLA_Adopter_Agreement.pdf).

<sup>18</sup> *Id.* at Exhibit B Audiovisual, Part 2: Compliance Rules for Source Functions § 3.1 at B-17.

The comments of AT&T suggest that, because of its content agreements, it would be required to mark all content from an AllVid adapter “Copy Never” because any third-party’s digital video recorder would be “out of AT&T’s control.”<sup>19</sup> As described above, this is a fundamental misunderstanding of how DTCP protection works. DTCP always has ensured both that consumers have the ability to copy any content marked “Copy One Generation” and that content owners can be assured that any copy made by the consumer will be protected against further copying or unauthorized retransmission.<sup>20</sup> Pursuant to DTCP’s combination of technological and licensing protections, any digital video recorder that is a licensed DTCP sink would be capable of protecting Copy One Generation content delivered by AT&T services, and would not record content marked Copy Never.<sup>21</sup> Thus, AT&T can and should continue to mark content to be delivered through the AllVid adapter in a manner consistent with the Encoding Rules.

Thus, consumer privileges of networking, time-shifting, and recording will be fully implemented and respected. Content owners that authorize encoding using DTCP understand that their content will be fully protected in accordance with the Encoding Rules. There is no need for any MVPD to exercise control downstream from the AllVid adapter over DVRs and other devices that receive MVPD content, or to move recording

---

<sup>19</sup> See Comments of AT&T at 35.

<sup>20</sup> The statements in the DLNA whitepaper quoted by AT&T refer only to what is specified in the DLNA guidelines. *Id.* at 35 n.44. Importantly, nothing in the DLNA guidelines prohibits any MVPD or content owner from marking content as Copy One Generation, or affects in any way what additional protections can be enabled using DTCP apart from what the DLNA guidelines provide. Thus, AT&T can encode content consistent with the Encoding Rules, and be confident that these copy protection instructions will be respected thereafter.

<sup>21</sup> As noted *supra* at 9, these recorders can use any of the technologies specifically approved by DTLA and any “bound” recording method.

capabilities to an AllVid adapter. Either of these results would harm competition from third party navigation devices; and, by extending an MVPD's reach downstream into the network, would frustrate the AllVid goal to create a robust interoperable home network under the control of the consumer, rather than the MVPD.

**B. DTCP Flexibly Supports Additional MVPD and Content Owner Business Models.**

Contrary to the assumptions of certain commenters, DTCP does carry information that will support additional MVPD business models. Some of those capabilities have been in place for several years; others are in process; and still others can be accommodated with input from content owners and MVPDs.

**1. DTCP Can Support Video Rental Models.**

A few comments erroneously suggest that DTCP could not support video rental capability.<sup>22</sup> In fact, *DTCP built support for video rental models into its Specification since 2001*. The DTLA Specification defines eight “retention” periods, per discussions with representatives of the motion picture industry, for retention of no less than 90 minutes, 3 hours, 6 hours, 12 hours, 1 day, 2 days, 1 week, and forever.<sup>23</sup> DTLA's licensing agreements require that access to the content be disabled after the defined period.<sup>24</sup> This “retention” information will be used by the technological methods

---

<sup>22</sup> See Comments of Charter Communications at 7-8; Comments of NagraVision at 8-9; *see also* Comments of DirecTV, Inc. at 17.

<sup>23</sup> DTCP Specification, Appendix B § B.2.1 at 67. The 90-minute retention period is a minimum requirement under DTLA's agreements, so that a consumer always has the right to “pause” Copy Never content (such as pay-per-view and video-on-demand programming) for in-home viewing convenience.

<sup>24</sup> Adopter Agreement, Exhibit B Audiovisual Part 1: Compliance Rules for Sink Functions § 2.1 at B-8; Exhibit B Audiovisual Part 2: Compliance Rules for Source Functions § 2.3 at B-16.

implemented by the DVR manufacturer to effectuate the rental model. The technological means to delete access to the content will vary with, and thus are the responsibility of, the storage technology used in the DTCP Licensed Product. Similarly, the means to charge rental fees and the amount of those fees will vary with, and must be supplied by the video service. By providing only the minimum information necessary to support rental rather than a full end-to-end DRM, DTCP helps to promote innovation: manufacturers and MVPDs are free to develop and choose among technologies that best support their particular business models, and can continue to improve their rental services without any constraint from DTCP.<sup>25</sup>

The DTCP Specification also notes, “[i]f an inter-industry standard or consensus supports retention states that differ from those set forth in this Specification, then this Specification may be amended or supplemented to reflect such consensus retention states.”<sup>26</sup> Thus, DTLA is willing to revise these settings in response to industry consensus and input as to what different or additional rental times might be desirable to support an MVPD-delivered rental model, or to discuss whether reliance on some other datum (such as a relative or hard date function) is preferable. Given the interest that certain commenters have expressed in facilitating a rental model, DTLA suggests this

---

<sup>25</sup> DTLA’s approach to carry information to enable interoperability between protection technologies is thus consistent with promotion of innovation in new business models and the content protection methods that support them. *See* Comment of Motorola at 18, n.58.

<sup>26</sup> DTCP Specification, Appendix B § B.2.1 at 67, n.54. Devices unable to support the precise periods indicated by the DTCP Retention field are required under the Adopter Agreement to respect the next more restrictive setting. Adopter Agreement, Exhibit B Audiovisual Part 2: Compliance Rules for Source Functions § 2.3 at B-16.

could be an appropriate time to convene a process to address those settings. DTLA would be pleased to participate in that process.

2. DTCP Can Support New Services, such as those Defined in the MPAA Waiver Order.

As DTLA also informed the Commission, DTCP can support “selectable output control” capability pursuant to the waiver granted by the Media Bureau to the MPAA.<sup>27</sup> This capability will enable MVPDs to offer consumers early-window access to view theatrical motion pictures. DTLA is finalizing revisions to its Specification that will enable implementation of a “Digital Only Token” that will identify content permitted to be output only from protected digital outputs, for limited purposes.<sup>28</sup>

3. DTCP Can be Adapted and Expanded to Support Additional Business Models.

---

<sup>27</sup> See *In the Matter of Motion Picture Ass’n of America, Petition for Expedited Special Relief, Petition for Waiver of the Commission’s Prohibition on the Use of Selectable Output Control*, (47 C.F.R. § 76.1903), CSR-7947-Z, MB Docket No. 08-82, Comments of DTLA (July 21, 2008).

<sup>28</sup> Content permitted to be encoded with the Digital Only Token consists of content permitted to be so output pursuant to the May 7, 2010 Waiver Order; or content permitted to be marked with the AACS Digital Only Token, *see* Advanced Access Content System (“AACS”) Adopter Agreement, Exhibit E Part 3 § 1.2 at E-29, [http://www.aacsla.com/license/AACS\\_Adopter\\_Agrmt\\_090619.pdf](http://www.aacsla.com/license/AACS_Adopter_Agrmt_090619.pdf). One comment noted the recent inclusion of an “Analog Sunset Token” in the DTCP Specification. *See* Comments of Dish Network/Echostar Technologies at 12; *see* DTCP Specification at 68. DTLA adopted this requirement in fulfillment of the obligations on all digital output protection technologies approved by AACS. *See* AACS Adopter Agreement, Exhibit E Part 2 § 2.2.1 at E-17. The DTCP Analog Sunset Token applies only to Decrypted AACS Content, in cases where the AACS licenses already do prohibit analog output. Thus, it should not affect broadcast or network content streamed by an MVPD through an AllVid adapter. *See* Adopter Agreement, Exhibit B Audiovisual, Part 1: Compliance Rules For Sink Functions §§ 2.1-2.2, 4.7, at B-8, B-12-13. While DTLA, as a matter of course, has the ability to expand the definition of Analog Sunset Content in response to any future market requirements, it has neither any obligation nor any present intention to do so.

Further, DTLA collaborates with MVPDs and content owners to enhance protection and/or carry information so as to support additional business models and device capabilities. DTLA has addressed many past requests, and remains willing to do so in the future.<sup>29</sup> If, as suggested in the comments of DirecTV,<sup>30</sup> MVPDs or content providers desire additional fields (such as expiration dates), DTLA is willing to collaborate to meet their needs; and DTCP should not interfere in any way with the ability of MVPDs to accommodate the making of new offers to consumers, or billing and collection capabilities.

DTLA therefore disagrees with the assumptions made by certain commenters that DTCP lacks necessary flexibility, and invites them to discuss whether and how DTCP can address their specific concerns.

**C. DTCP Can Support Required DRM Systems for Advanced Services.**

A few comments incorrectly suggested that DTCP does not or cannot support DRM implementations.<sup>31</sup> As noted above, DTCP currently is interoperable with several

---

<sup>29</sup> For example, in response to requests from content owners, MVPDs and Adopters, in addition to those Specification additions identified above, DTLA has included and is working on capabilities such as: additional localization to support home and personal networking; protection for automotive-based systems; support for Internet Protocol; a method to enable the making of a specified number of copies from transmitted content (“Copy Count”); ability to retrieve content usage rules in format non-cognizant devices; and the ability to access protected content from the home network in remote locations.

<sup>30</sup> Comments of DirecTV at 17.

<sup>31</sup> See Comments of AT&T at 33-35; Comments of Dish Network/Echostar Technologies at 11-12; Comments of MPAA at 5-6. These comments are made in the abstract, and do not identify particular DRM mechanisms that they contend cannot interoperate with or be supported by DTCP, or what additional functions they desire DTCP to facilitate. Nor did they define what technologies or functionalities are necessary to constitute, in their view, a DRM system appropriate for each of the various types of MVPD-delivered content. Nor do they suggest why a high level of DRM

content management technologies for storage and transmission functions, and has other requests for interoperability approval in process. Many of these technologies would be classified as “DRMs.” Thus, as noted above, the combination of technologies tied together by DTCP, from a conditional access delivery system through to protections for output, display, storage, and moving of content, together can constitute a complete system for digital rights management.

DTCP already is complementary to “domain-based” systems<sup>32</sup> in that DTCP can be both an authorized input to and an authorized output from a domain-based system. Mapping and interoperability issues can be discussed with the proprietors and proponents of any domain-based systems, as DTLA has done for all other interoperability requests.<sup>33</sup> In addition, as noted in other contexts in this Reply, DTCP is flexible enough to be adapted in other ways to enable it to function as part of a domain-based system, and DTLA is prepared to work with proprietors and proponents of such systems to mesh DTCP with their particular protection systems.

---

protection is necessary or appropriate for time-shift recording, which covers the vast majority of content delivered by an MVPD.

<sup>32</sup> A recent *ex parte* notice referred to the digital rights management capabilities of the European Digital Video Broadcast CPCM technology. See Letter from Alicia W. Smith, The Smith-Free Group, L.L.C. to Marlene H. Dortch, Secretary, FCC, MB Dkt. No. 10-91 (July 1, 2010). CPCM was proposed for the DLNA content protection guidelines, but was not accepted. DTLA is unaware of any actual deployment of CPCM anywhere in the world.

<sup>33</sup> Several comments observe that DLNA is in process of completing its DRM guidelines. But, as noted above, this does not affect the ability of DTCP to facilitate recording of protected content in accordance with the content owner’s requirements and the Encoding Rules. Moreover, there is every reason to expect that the ongoing inter-industry DLNA process, whose active membership includes representatives of the motion picture, MVPD, and consumer electronics and information technology industries, can and would develop any standards necessary to accommodate digital rights management techniques for the AllVid environment..



### **III. DTCP Provides Robust Protection for MVPD-Delivered Content.**

One commenter raised the question as to how to address a potential technological crack of DTCP.<sup>34</sup> This concern is by no means unique to DTCP. The question is pertinent for any protection system that might be used to protect content on a home network because, in plain fact, no technology is immune from cracking. Commercial “pirates” bent on breaking content protection undoubtedly can find ways to defeat any and every DRM and protection measure. Notwithstanding, DTCP believes the Commission should consider several key points.

First, where consumers can enjoy their reasonable and customary use of content, there is less incentive for attack. DTCP accommodates those consumer rights and privileges. Under the DTCP Encoding Rules, consumers always can make a first generation of copies of subscription programming and can “move” those copies between devices; pause on-demand and pay-per-view content for periods from a minimum of 90 minutes to 1 week; and stream and share live and recorded protected content throughout the home network. Terrestrial broadcast channel content is not protected with DTCP. Because DTCP facilitates these consumer use cases, most consumers will never know DTCP is there.

Second, DTCP-IP is a robust technology. DTCP-IP uses AES 128 encryption, which has been proven to provide effective protection in numerous commercial implementations. Pursuant to content owner license requirements, DTCP currently is

---

<sup>34</sup> Comment of Dish Network/Echostar Technologies at 13. The commenters suggest that the Commission can and should foster policies that promote consumer flexibility and thereby reduce the incentive to defeat protection technologies. *Id.* DTLA agrees.

being used effectively and extensively on a number of platforms and devices, and in a number of world markets.

Third, regardless of what protection technology may be used on the home network, the Commission and commenters should keep in mind that consumers receive, via the AllVid adapter, access to content for which they have already paid. Historically, the goal for protecting lawfully-acquired content is to put technical barriers, and legal protections against circumvention of those barriers, in the way of actions that would break the rules; simply stated, to “keep honest people honest.” As a result, of even those few consumers who may try to evade the rules, the vast majority quickly will give up (although, as noted above, we and content owners fully understand that dedicated security crackers have the time, skill, and tools to defeat any technology). DTCP and the technologies approved for output and storage of DTCP-protected content more than meet this standard.

Finally, it is possible to respond to attacks against protection technologies. The impact of a particular attack may vary. For example, some attacks can only be accomplished with a high level of personal skill or specialized tools unavailable to most consumers and, so, would have less potential impact on the market than a more widespread break. Moreover, the potential gain from an attack may not be justified by the economic costs in time, effort, and equipment. DTLA, like any responsible protection technology proprietor, would be prepared to address a meaningful attack

promptly and in a manner that would not disenfranchise or harm those consumers who follow the rules.<sup>35</sup>

## CONCLUSION

DTLA appreciates the comments supporting the potential role of DTCP in a home network that obtains MVPD content via an AllVid adapter. DTLA remains willing and able to work with content owners, MVPDs, Adopters, and the Commission to make certain that DTCP-IP enables the AllVid adapter to give consumers access to the services they want, in a manner that supports home and personal networking and reasonable and customary recording. We thank the Commission for this opportunity to explain in greater detail the nature and operation of DTCP, and to reply to questions raised in various comments. Should the Commission have any additional questions, we would be pleased to respond to them.

---

<sup>35</sup> We address, briefly, two other comments. First, Dish/Echostar noted the existence of a provision in the Adopter Agreement relating to non-interference with an audiovisual watermark. *Id.* at 12, Exhibit B Audiovisual, Part 1: Compliance Rules for Sink Functions § 6, at B-13-14. This provision has been in DTLA’s licenses since 2001, but no “consensus watermark” has been selected by the affected industries and the provision is not in effect. If the requirement were ever to become effective, it is limited to an obligation not to knowingly and intentionally interfere with the mark (*e.g.*, to strip or damage it in the content); and does not prevent Adopters from incorporating consumer-friendly product features such as zooming, scaling, cropping, picture-in-picture, format shifting, downsampling, etc., that inherently could affect the mark. *Id.*, § 6.3 at B-14.

Second, in response to comments of Beyond Broadband Technology, LLC, there is no heightened risk from key generation. *See* Comments of Beyond Broadband Technology, LLC at 15-16. Generation of public/private key pairs has been common cryptographic practice for several decades, and has created little risk to anyone. DTLA retains the services of a secure facility to generate public/private key-certificate pairs, and a separate administrator to maintain information on which keys were assigned to particular Adopters. This information would be used in case certificate revocation were required (to date, no revocations have occurred). DTLA’s Founders obtain only aggregate information concerning the number of generated keys.

Date: August 12, 2010

Respectfully submitted,

*MBA /s/*

*SDG /s/*

Michael B. Ayers  
President  
Digital Transmission Licensing  
Administrator, LLC  
949.461.4715  
Michael.Ayers@tais.toshiba.com

Seth D. Greenstein  
Constantine Cannon LLP  
1301 K Street NW, Suite 1050 East  
Washington, D.C. 20005  
202.204.3514  
sgreenstein@constantinecannon.com