

**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
)	

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

Date: July 13, 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

	Page
<u>SUMMARY OF DTLA COMMENTS</u>	ii
<u>I. BACKGROUND OF DTCP TECHNOLOGY</u>	2
<u>A. DTLA AND DTCP</u>	2
<u>B. HOW DTCP PROMOTES INTEROPERABILITY ON HOME NETWORKS</u>	3
<u>C. DTCP-IP IS LICENSED ON REASONABLE AND NONDISCRIMINATORY TERMS.</u>	6
<u>II. HOW DTCP CAN PROTECT CONTENT OUTPUT FROM AN ALLVID ADAPTER</u>	8
<u>III. AUTHENTICATION FROM THE ALLVID ADAPTER UPSTREAM TO THE MVPD SYSTEM IS, AND SHOULD BE, SEPARATE FROM DTCP AUTHENTICATION OF THE HOME NETWORK.</u>	11
<u>CONCLUSION</u>	14

SUMMARY OF DTLA COMMENTS

The Digital Transmission Licensing Administrator, LLC (“DTLA”), the developer and licensor of the Digital Transmission Content Protection (“DTCP”) technology, supports the proposal for an AllVid adapter, and believes DTCP can play a constructive role in that gateway device. For audiovisual content acquired or accessed by a consumer in protected formats, DTCP perpetuates protection for that content when transmitted across the links between devices connected over high-speed bidirectional digital home networks. DTCP has been widely implemented in digital entertainment products, including MVPD-supplied set-top boxes, Blu-ray disc players and digital video recorders, and is included in the DLNA guidelines for networking audiovisual products.

DTCP-IP is well suited to provide protection for content output from an AllVid adapter to the home network. DTCP-IP assures that protected content will be passed only to devices that authenticate compliance with DTCP for copying and retransmission to the network in accordance with the Commission’s Encoding Rules. DTCP will not affect content such as terrestrial broadcast programming that is not subject to protection under the Commission’s Encoding Rules. DTCP is interoperable with other commonly-used content protection technologies, such that content protected with DTCP can be reprotected using other technologies, and vice versa. DTLA licenses DTCP on fair, reasonable, and nondiscriminatory terms. DTCP is flexible enough to accommodate new business models offered by MVPDs, and can be adapted to address future requirements.

DTCP would not perform separate conditional access or security functions between the AllVid adapter and the MVPD. Conversely, authentication by the AllVid adapter of devices on the network should be performed by DTCP, and not by the MVPD.

**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

**Comments of Digital Transmission Licensing Administrator LLC
To “AllVid” Notice Of Inquiry**

The Digital Transmission Licensing Administrator LLC (“DTLA”) submits these Comments in response to the Notice of Inquiry (“NOI”) in the above-referenced docket proceedings, published in 75 Fed. Reg. 27264 (May 14, 2010). DTLA’s technology development efforts focus on the promotion of home networking of protected audiovisual content acquired through and stored on a variety of consumer electronics and information technology entertainment products. DTLA strongly supports the Commission’s efforts through the National Broadband Plan, the Fourth Further Notice of Proposed Rulemaking, and now this NOI to promote digital home networking of content received from an MVPD to competitive navigation, storage, and display devices. DTLA comments below on the content protection aspects of the proposed “AllVid” adapter or gateway solution.

I. Background of DTCP Technology

A. DTLA and DTCP

DTLA consists of five founding companies: Intel Corporation, Hitachi, Ltd., Panasonic Corporation, Sony Corporation, and Toshiba Corporation, also known collectively as “5C.” As a result of an inter-industry technology review project of the Copy Protection Technical Working Group, in 1998 these founders together created the Digital Transmission Content Protection technology “DTCP” as a simple and inexpensive method, affording a high degree of protection, to protect copyrighted commercial entertainment content transmitted over high-speed bi-directional digital interfaces.

Certain content is made available to consumers in protected form, such as via MVPD conditional access systems or on optical discs using encryption techniques. DTCP perpetuates that protection within the home and personal network by transmitting that content, in encrypted form, only to devices along the home network that have authenticated compliance with DTCP. In this way, DTCP provides content owners with robust protection against unauthorized copying, interception, tampering, or retransmission, while ensuring that consumers retain the ability to view and store protected content on their home networked devices. DTCP enables the same content stream to be delivered simultaneously to multiple display and storage devices, and provides consumers the flexibility to move copies of protected content among devices on the home and personal network.

DTCP has been licensed by more than 140 companies, including manufacturers of television receivers, cable set-top boxes, and digital recorders; IT companies; MVPD

system operators; semiconductor manufacturers; and component resellers. Three major motion picture companies have signed agreements to be DTCP Content Participants.¹ Numerous digital television products currently on the market, including high definition digital television sets, digital recorders, Blu-ray Disc players, and cable set-top boxes, utilize DTCP for protection of digital audiovisual outputs. DTCP is required by Commission regulations in the network-capable outputs of all High Definition set-top boxes deployed by CableLabs's MSO owners, and DTCP over IP and IEEE 1394 are approved to protect outputs of plug-and-play boxes under the various CableLabs licenses.

B. How DTCP promotes interoperability on home networks

DTCP protects the transmission link between devices on a home or personal network. As a "link protection method," DTCP facilitates interoperability among devices along a home network, including devices that may use different content protection systems for storage or retransmission.

DTCP can be mapped to protect with equal effectiveness audiovisual content transmitted over any high-speed bi-directional transport. Currently, DTCP has been mapped for use over Internet Protocol, Wireless HD, IEEE 1394, MOST and IDB-1394 transports for mobile environments, USB, Bluetooth, and Op-iLink. DTCP-IP can be

¹ The three are Sony Pictures Entertainment, Warner Bros., and the Walt Disney Company. Content Participants obtain benefits such as the ability to review and object to changes to DTCP that would materially and adversely affect its integrity and security (known as "change management" rights) and to assert third party beneficiary rights under the Adopter Agreement. Content owners also may protect their commercial entertainment works using DTCP without signing any agreement and without charge, pursuant to the "IP Statement" issued by DTLA. *See* http://dtcp.com/documents/licensing/IP_Statement.pdf.

used for numerous physical or wireless interfaces (including Ethernet and 802.11).² In each instance, the process of mapping incorporates all elements of protection offered by DTCP, and conveys the usage and rights information specified for that format. Thus, DTCP protects content equally robustly regardless of the protocol over which the protected content travels.

Content protected with DTCP can be re-protected with other content protection systems. DTCP passes to other protection systems the content control information incorporating usage and encoding rules associated with the source content (with respect to the level of permissible copying, retention or retransmission). DTCP will enable this “hand-off” of protected content only to those systems that meet both technological and legal requirements at least as stringent as those adopted by DTCP.³ DTCP similarly can re-protect content previously protected by other systems, and implement the defined usage rules in DTCP-protected transmissions. It thus is unnecessary for DTCP to identify whether that content originated from a particular source, such as from a DVD or Blu-ray disc, subscription cable channel, or video-on-demand service. What matters from a

² DTCP-IP uses the AES-128 encryption method as its standard “baseline” cipher. To thwart attempts to encapsulate DTCP-protected content within another network transport and then retransmit such content outside the home network, DTLA developed for DTCP-IP a series of localization requirements, using the Time-To-Live (“TTL”) and Round Trip Time (“RTT”) elements of the Internet Protocol. Though DTLA was the first to define such localization requirements, the RTT requirement since has become standard techniques used in other DTCP protocols as well as by other content protection technologies.

³ DTLA approves digital output and recording technologies according to criteria that assure the technologies are robust, and that licenses to these technologies include Compliance Rules and Robustness Rules no less stringent than those imposed by DTLA. See <http://dtcp.com/approvedtechnologies.aspx> for a current list of those approved technologies. DTLA remains willing to work with the proprietors of other technologies to make content protected with DTCP available to be protected with those systems and/or vice versa. DTLA has not refused any request to enable such interoperability.

content protection perspective is that the content remains fully protected according to the usage and encoding rules established by the content owner.

Because DTCP is mapped to many protocols and content protection systems, it serves as a *lingua franca* to convey protected content and related rights and usage data between interoperable formats and devices.⁴ DTCP thus complements and coexists with current copy protection technologies, including conditional access systems for digital television transmission and peripheral display and recording devices, and can be kept compatible with protection technologies that may be developed in the future.

DTCP has won inter-industry support as an output protection technology for DVD,⁵ high definition optical media,⁶ cable⁷ and satellite television, and recently for the “Freeview HD” system in the United Kingdom.⁸ In July 2006, the Digital Living

⁴ In addition, the DTLA Adopter Agreement permits use of “bound” copy protection methods without DTLA approval, if the recorded content is encrypted, cannot be re-copied, and can only be played on the device that made the recording. *See* DTLA Adopter Agreement, Exhibit B Part 1: Compliance Rules for Sink Functions, § 2.2.1.2, http://dtcp.com/documents/licensing/DTLA_Adopter_Agreement.pdf.

⁵ *See* CSS Procedural Specifications, DVD Copy Control Association (Version 2.8 August 10, 2005), § 6.2.1.2, approving DTCP-IP for all transports, and DTCP for 1394, MOST, and IDB-1394.

⁶ *See* Advanced Access Content System (“AACCS”) Adopter Agreement, at Table D-1, at E-61, http://www.aacsla.com/license/AACS_Adopter_Agrmt_090619.pdf, approving use of DTCP over all protocols.

⁷ *See* <tru2way> Host Device License Agreement, Exhibit C Compliance Rules § 2.4; Amended and Restated Nonexclusive CableCARD-Host Interface License Agreement, Exhibit C “Compliance Rules” § 2.4.1; DCAS Host License Agreement, Exhibit C “Compliance Rules” § 2.4.1., <http://www.cablelabs.com/opencable/documents>.

⁸ Ofcom, “Statement on content management on the HD Freeview platform,” (June 14, 2010), http://stakeholders.ofcom.org.uk/binaries/consultations/content_mngt/statement/statement.pdf

Network Alliance (“DLNA”) adopted DTCP-IP as a content protection technology for home networks compliant with its inter-industry voluntary standards.⁹ DTCP (including DTCP-IP) is an approved output protection technology for entertainment content received on a wide range of devices, including cell phone-based devices, that use Open Mobile Alliance DRM 2.0.¹⁰ The RVU Alliance standards include DTCP-IP as the content protection method.¹¹

Beyond question, DTCP (including DTCP-IP) has been widely recognized as effective technologies that provide robust protection for audiovisual content of all types – high-definition and standard definition, from basic cable programming to commercial discs and pay-per-view events. Over years of experience, DTLA has proved in practice that content protected with DTCP remains well protected when “handed off” downstream to devices that use or rely on other protection methods.

C. DTCP-IP is Licensed on Reasonable and Nondiscriminatory Terms.

The NOI asks in paragraph 32 whether intellectual property rights required for the AllVid adapter would be available on reasonable and nondiscriminatory terms. DTLA licenses the technology owned by DTLA and its founders that is necessary to implementation of the DTCP Specification on a fair, reasonable and nondiscriminatory basis.

⁹ See DLNA Networked Device Interoperability Guidelines, August 2009; DLNA Overview and Vision White Paper 2007 at 18, http://www.dlna.org/en/industry/pressroom/DLNA_white_paper.pdf.

¹⁰ See CMLA Client Adopter Agreement, Table Y1, CMLA Authorized Digital Outputs at 55-56 (Dec. 18, 2009), <http://www.cmla.com/documents/CMLA%20Client%20Adopter%20Agreement.pdf>.

¹¹ See RVU Alliance, http://www.rvualliance.org/about_rvu.

DTLA's agreements follow the approach, common to many content protection technology licenses, of licensing all "Necessary Claims" owned by the founders in the technology.¹² All Adopters and all Content Participants are offered the same terms under their respective licenses.¹³ Any later amendment to the licenses is offered retroactively to all prior licensees.

Prospective Adopters can download from the DTLA website non-confidential versions of the Specification for review before signing the licenses.¹⁴ Adopters can sign first as an "Evaluator," to evaluate the full confidential version of the Specification and enable internal development using facsimile keys (subject to a lower payment and non-disclosure obligations). Evaluators can file an Activation notice to obtain access to production keys and to permit manufacture and distribution of DTCP-compliant products.

Licenses to encode or to cause to be encoded content with DTCP are available to any content owner in two ways. Major content owners may execute a Content Participant Agreement with DTLA; or, any content owner can benefit from the DTLA "IP

¹² The definition of "Necessary Claims" is specified in the DTLA Adopter Agreement at Section 1.22, and in the DTLA Content Participant Agreement. The agreements grant "a nonexclusive, nontransferable, nonsublicenseable, worldwide sublicense under the Necessary Claims of the Founders, as well as under any trade secrets or copyrights embodied in the Specification to make, have made, use, import, offer to sell and sell Licensed Products and Licensed Components... ." DTLA Adopter Agreement, Section 5.2; *cf.* Content Participant Agreement, Section 2.1 (granting a similar scope of rights with respect to encoding of DTCP).

¹³ These licenses are available for review and download from the DTLA website, at <http://dtcp.com/agreements.aspx>.

¹⁴ See <http://dtcp.com/specifications.aspx>.

Statement,” which allows encoding of content for DTCP protection without payment so long as the content owner observes the DTLA Encoding Rules.¹⁵

II. How DTCP Can Protect Content Output from an AllVid Adapter

DTLA believes that DTCP can perform a necessary role in an AllVid adapter to promote secure transmission and interoperability across the home and personal network of MVPD-delivered conditional access content with other audiovisual content acquired by consumers. As DTLA envisions the operation of the AllVid adapter, the adapter will perform conditional access to ensure consumers can receive those channels to which they have subscribed. Functions such as device discovery, channel selection, remote signaling, networking, and upstream communications can be addressed through the DLNA and UPnP standards developed cooperatively by representatives of all affected industry segments.

DTLA envisions DTCP on an AllVid adapter operating much in the same way as DTCP operates in MVPD set-top boxes and other products today. The owner or licensor of particular audiovisual content would require by contract the application of DTCP to particular transmitted programming. That contractual requirement would be perpetuated through to the MVPD, which would be responsible for properly encoding DTCP in its program streams. Content control information in the program stream will signal whether and how DTCP is to be applied. DTCP would be applied to content in accordance with the Commission’s (and DTLA’s) Encoding Rules.¹⁶ Consequently, for example, subscription programming over channels such as HBO or Showtime could be marked

¹⁵ *Supra at 3 n.1.*

¹⁶ *See 47 C.F.R. § 76.1901 et seq.; DTLA Content Participant Agreement Section 5.4, http://dtcp.com/documents/licensing/DTCP_Content_Participant.pdf.*

“Copy One Generation,” and content delivered via pay-per-view or video-on-demand could be encoded “Copy Never.” Programming such as MVPD carriage of terrestrial broadcast television programming would not be encoded with DTCP, and the application of DTCP to other content would not affect in any way the networking of any content to which DTCP is not applied.

The DTCP “sink” module at the output of an AllVid adapter would perform authentication and key exchange processes with the DTCP “source” modules of the other network devices requesting access to that content. If those processes succeed, the content will be encrypted using AES-128 and transmitted across the network so as to be available to all other authenticated devices on the network.¹⁷ The DTCP source devices will follow the usage rules set forth in the accompanying copy control information. Those authenticated devices also may output and/or store such content using any of the digital protection technologies authorized under the Adopter Agreement. *Supra*, at 4-5 and n.4. As a result, content received from an MVPD would be available to the home network, along with other content available to the consumer such as from DVR or PC storage devices, a home media server, an internet website, or a service provider.

DTCP currently accommodates all types of conditional access video content delivered over MVPD services, including subscription channels, subscription on-demand, video-on-demand, and pay-per-view services. DTCP also can protect content delivered in new business models, such as the contemplated service made possible by the

¹⁷ Under the DTCP Specification, up to 34 authenticated sink devices (including bridge devices) may receive a particular DTCP-protected content stream at any time. Digital Transmission Content Protection Specification Volume 1 v.1.6 Appendix C (Mar. 19, 2010) http://dtcp.com/documents/dtcp/Info_20100319_DTCP_V1_1p6.pdf (hereinafter “DTCP Specification”).

Commission's recent selectable output control waiver Order.¹⁸ DTCP long has provided for additional functionality such as the ability to retain Copy Never content for defined periods of time (*e.g.*, so as to promote rental or subscription services as well as to enable a consumer to “pause” content).¹⁹ Additional or different retention periods can be defined as well. DTLA soon will release specification changes that will add, among other things, a “Copy Count” function to enable the making of a specified number of copies of certain types of content. Further, DTLA can adapt DTCP to carry additional content management information, or incorporate additional capabilities and rules.

DTLA believes it is appropriate for the Commission to provide for the use of DTCP-IP as part of the interoperability “suite” for the AllVid adapter. The DLNA guidelines, including needed standards such as UPnP in addition to the DTCP-IP protection technology, provide both MVPDs and competitive device manufacturers with assurance that devices connected to the AllVid adapter will correctly interoperate, such that MVPD-delivered content and services can be integrated into the home and personal network. DTLA therefore supports a requirement for the AllVid adapter to support DLNA, including DTCP-IP.²⁰

¹⁸ *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 (May 7, 2010). *See* Comments of DTLA in that proceeding (July 21, 2008).

¹⁹ *See* DTCP Specification at 67.

²⁰ Notwithstanding, DTLA notes that the ability of DTCP-IP to interoperate with approved technologies facilitates seamless interchange of data between devices that may use different systems. Thus, for DTCP-IP to play a constructive role in integrating the AllVid adapter into the home network, DTCP-IP does not have to be the only accepted protection system.

III. Authentication from the AllVid Adapter Upstream to the MVPD System Is, and Should Be, Separate from DTCP Authentication of the Home Network.

In paragraph 28 of the NOI, the Commission reviews issues relating to the authentication capabilities of DTCP. An AllVid adapter would be required to validate itself both upstream to the MVPD, and downstream with other devices on the network. However, each of these is a separate function with a different purpose. The former is a function of conditional access security that does not implicate DTCP. The latter is the same type of authentication that every DTCP source device must perform to ensure that protected content only is transmitted to devices that authenticate compliance with DTCP-IP. DTLA explains below the different types of authentication relevant to the AllVid adapter, and different revocation needs.

As noted, an AllVid adapter will need to incorporate technologies that perform the MVPD's conditional access security functions. These functions generally address MVPD concerns with preventing theft of service or harm to the network. Conditional access technologies need not be uniform across all adapters. Each MVPD can select and implement a technology that comports with its security needs and system requirements. Each such method is likely to include a method whereby the MVPD will validate the adapter and identify the services which that subscriber is entitled to receive. This process occurs between the adapter and the MVPD network, upstream from the output of the adapter to the home network.

The next step is to assure that content that the subscriber lawfully acquires via a conditional access system remains protected within the home according to the content provider's instructions and the Commission Encoding Rules. DTCP authentication

provides that protection downstream from the AllVid adapter to all devices on the subscriber's home network that can perpetuate protection for that content. The authentication process verifies which devices include DTCP protection, and uses the keys from those devices to encrypt the transmitted content and transmit the content in a secure authenticated channel on the network.

DTCP authentication relies on certificates and keys generated by the DTLA's certificate authority and distributed to DTCP Adopters. Each DTCP-compliant device has a single device certificate. It is likely that AllVid adapters would perform authentication using a unique key and certificate per device.²¹ The device certificate of a particular product can be revoked, on a device-by-device basis, under the criteria and procedures in the DTCP license agreements.²² During the authentication process, the DTCP source device will determine whether the certificate of any of the requesting sink devices is on

²¹ The DTLA agreements also provide for another category of keys and certificates, known as "common device keys." As the name implies, a "common" key uses the same value in potentially a large number of applications. The typical intended use of a common key occurs where DTCP is enabled via a software-based application on a multi-functional product. It thus is unlikely that a common key would be used in an AllVid adapter. If an Adopter elected to use a common key for the Adapter, it would follow the requirements set forth in the DTLA Adopter Agreement Procedural Appendix 2.2(ii). In summary, the application must be implemented in software or firmware, and the Adopter must be able to replace the common key by remote upgrade in case of revocation. Revocation would be performed only in conjunction with replacement of the common key, so that the Adopter has the flexibility to implement revocation in a manner that will not inconvenience any consumer.

²² See DTLA Adopter Agreement, Section 4; DTLA Content Participant Agreement, Section 6. Under these agreements, revocation of a DTCP certificate may be undertaken for limited reasons, generally relating to the loss, theft, or misuse of the certificate. DTLA notes that it has not had any cause or requirement to revoke a unique device certificate.

the most current certificate revocation list, and will not transmit DTCP-protected content to any device with a certificate on the list.²³

In sum, the MVPD conditional access technologies, and not DTCP-IP, would be used to validate the AllVid adapter upstream to the MVPD system. However, the MVPD does not need to authenticate the AllVid adapter to other devices on the home network. That function can be performed using DTCP-IP.

²³ DTCP revocation will not affect the ability of networked devices to obtain access to content that has not been protected by DTCP.

Conclusion

DTLA supports the Commission's proposal for an AllVid adapter or gateway for MVPD-supplied content to the home network. DTLA believes that DTCP-IP can play a constructive and necessary role in the transmission and exchange of protected content downstream from the adapter across the network. We encourage the Commission to consider DTCP-IP as part of a suite of technologies to support the AllVid approach. Should the Commission have any questions about these Comments or any matters relating to DTCP or to the NOI, please feel free to contact the undersigned at your convenience.

Date: July 13, 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