

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

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

**Comments of Digital Transmission Licensing Administrator LLC  
To Fourth Further Notice Of Proposed Rulemaking**

The Digital Transmission Licensing Administrator LLC (“DTLA”) submits these Comments in response to the Fourth Further Notice of Proposed Rulemaking (“FNPRM”) in the above-referenced docket proceedings, published in 75 Fed. Reg. 27256 (May 14, 2010). DTLA commends the Commission’s efforts through this FNPRM to promote digital home networking of audiovisual content through retail availability of competitive navigation devices. DTLA submits these Comments in support of the proposed additions to the interface regulatory requirements between navigation devices and the home and personal network.

**Background on 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.” 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.

In overview, DTCP perpetuates protection within the home and personal network of content received by the consumer in a protected form (*e.g.*, an encrypted optical disc or via a conditional access system). DTCP enables the protected output of this content only to those devices along the home network that have authenticated compliance with DTCP. In this way, DTCP provides content owners with protection against unauthorized

copying, interception and tampering within the home, while ensuring that content can be viewed and copied on home networked devices.

Currently, DTCP is mapped to a number of interface protocols including Internet Protocol (“IP”), IEEE 1394, USB, and Wireless HD. DTCP-IP can be used for numerous physical or wireless interfaces, including all of the physical interfaces listed in the FNPRM. DTCP also can be mapped directly to a protocol format as a “native” implementation. 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. Moreover, 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.<sup>1</sup>

### Comments on Interface Requirements

DTLA supports the Commission’s proposal to modify the interface requirements in Rule 76.640(b)(4)(ii). When that Rule first was adopted in 2003, only two interfaces were available in the market with applied content protection technology (as required by cable operators and content licensors). Of those two only IEEE 1394 with DTCP facilitated consumer recording or connection to a home and personal network. Since that time, additional interfaces have become increasingly popular for use in home networking applications. DTLA believes that expanding the list of interfaces will give device manufacturers, cable operators, and consumers greater choice in how best to integrate home networking into their products.

To the extent that content protection will continue to be required for certain content flowing over these interfaces, DTCP can meet that requirement. DTCP-IP can be implemented over all of the listed physical interfaces (including Ethernet, USB 3.0, Wi-Fi, and IEEE 1394). DTCP initially was mapped in native format to IEEE 1394. DTLA also had mapped DTCP to USB 2.0 in its native format[; and, in response to requests from our Adopters, DTLA will complete development of the native USB 3.0 implementation].

Because DTCP already has been mapped to protocols that operate over these and other interfaces, DTCP can facilitate interoperability among devices that rely upon any of the supported interfaces for input and output of protected video content. Moreover, should the Commission determine to permit additional interfaces, or if other interfaces gain marketplace acceptance, DTCP is flexible enough to be mapped to such other protocols and interfaces. DTLA would be interested in providing such support.

---

<sup>1</sup> DTCP extends substantial effort to enable interoperability with other systems for protected output or persistent storage of audiovisual content. *See* <http://dtcp.com/approvedtechnologies.aspx> for a current list of those systems. 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 further agrees with the Commission’s proposal to enable bidirectional communications of remote-control commands from networked devices over permitted network-capable interfaces. Among the many potential benefits, bidirectional communication could promote consumer-friendly capabilities supported by DTCP, such as the ability to move protected copies stored on one DTCP-enabled device to another DTCP-enabled device.

Comments on CableCARD Device Certification

In paragraph 18 of the FNPRM, the Commission proposes that CableCARD device certification be based upon testing only with respect to the procedures adopted by the Commission for unidirectional cable products, which would “streamline the device certification process while allowing the cable industry to continue to control its system security and prevent theft of service.” DTLA wishes to confirm its understanding that “theft of service” refers only to the controlled access delivery of content from the cable headend to the UDCP. It does not include any subsequent output of content from the UDCP to other devices or to the home or personal network. Thus, it does not apply to downstream content protection using DTCP, which neither is within the control of the cable service nor is intended to prevent theft of service. In that regard, DTLA confirms that CableLabs’s certification testing does not imply any certification from DTLA with respect to DTCP, and it is DTLA’s understanding that under the Commission’s proposed rule such testing would not be part of the CableLabs certification test requirements suite.<sup>2</sup>

Should the Commission have any questions about these Comments or any matters relating to DTCP or to the FNPRM, please feel free to contact the undersigned at your convenience.

Respectfully submitted,

*MBA /s/*

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

*SDG /s/*

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

---

<sup>2</sup> This Commission proposal appears to have been prompted in part by Comments from SageTV in NBP PN #27. DTLA submitted *ex parte* comments to certain statements made by SageTV in that proceeding. Our submission there reflected this same understanding, and so did not address any questions raised by SageTV with respect to the CableLabs certification process.