DOCKET FILE COPY ORIGINAL

DTLA Digital Transmission Licensing Administrator

Received & Inspected

MAR 1 2010

FCC Mail Room

February 23, 2010

ORIGINAL

Ms. Marlene Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

EX PARTE OR LATE FILED

Re: *NBP Public Notice #27, GN Docket No. 09-47,*
GN Docket No. 09-51, GN Docket No. 09-137, CS Docket No. 97-80

Dear Ms. Dortch,

The Digital Transmission Licensing Administrator LLC ("DTLA") submits these comments in response to the February 16, 2010 *ex parte* letter filed by SageTV, LLC in the above-referenced docket proceedings. Specifically, SageTV's letter made certain references to the technology licensed by DTLA, known as "DTCP," which we believe are inaccurate and require clarification. DTLA submits this brief response solely to address those points.

Background on DTLA and DTCP

The five founder companies of DTLA – Intel Corporation, Hitachi, Ltd., Panasonic Corporation, Sony Corporation, and Toshiba Corporation – are among the world's most prominent innovators in the fields of consumer video, computing and home networking technologies. As a result of an inter-industry technology review project of the Copy Protection Technical Working Group, in 1998 these five Founders (also known as "5C") together created the Digital Transmission Content Protection technology "DTCP" – 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.*, on 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 gives content owners protection against unauthorized copying, interception and tampering within the home, while ensuring that content can be viewed and copied on home networked devices.

No. of Copies rec'd 0+3
List ABCDE

DTCP is a "link protection" technology that helps secure the transmissions between digital entertainment products. DTCP "hands off" DTCP-protected content to other technological protection methods that will record that content in a protected format, or will transmit that content using a different protection method, so long as those methods perpetuate at least the same level of protection as required by the content owner using DTCP. In this way, DTCP acts as a kind of *lingua franca* that facilitates interoperability among devices of different manufacturers and different technologies.

DTCP's value to the home networking environment has been affirmed by the adoption of DTCP for Internet Protocol ("DTCP-IP") the Digital Living Network Alliance ("DLNA") inter-industry voluntary interoperability guidelines.[1] DTCP (including DTCP-IP) also 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.[2]

Inclusion of a functional IEEE 1394 interface with DTCP is required by Commission regulations for all High Definition cable operator-supplied set-top boxes.[3] DTCP-IP also has been approved by CableLabs to protect outputs of both cable operator-supplied boxes *and* plug and play set-top boxes under the tru2way, DFAST, PHILA, CHILA and DCAS licenses.

DTCP's licensing documents incorporate "encoding rules" that define the scope of protection that can be applied to specific types of audiovisual content (*i.e.*, copy freely, protected copying without numerical restrictions ("EPN"), copy one generation, and copy never). These DTCP encoding rules were supported by the cable and consumer electronics industries in the 2003 "Plug and Play" MOU as a model for what became the Commission's encoding rules applicable to MVPD content.[4]

---

1 *See* DLNA Interoperability Guidelines, October 2006; DLNA Overview and Vision White Paper 2007 at 18, available online at http://www.dlna.org/en/industry/pressroom/DLNA_white_paper.pdf Similarly, the now-disbanded High-definition Audio-video Network Alliance ("HANA") had selected DTCP under its voluntary inter-industry standards for home networking using IEEE 1394. *See* http://www.1394ta.org/about/HANA/index.html

2 *See* CMLA Client Adopter Agreement, Table Y1, CMLA Authorized Outputs at 55, http://www.cm-la.com/documents/CMLA%20Client%20Adopter%20Agreement.pdf (Dec. 12, 2009).

3 47 C.F.R. § 76.640(b)(i).

4 *In the Matter of: Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, Compatibility Between Cable Systems and Consumer Electronics Equipment*, CS Docket No. 97-80, PP Doeket No. 00-67, Second Report and Order and Second Further Notice of Proposed Rulemaking ¶ 54 (Oct. 9, 2003) (the "Plug and Play Order"). *See* 47 C.F.R. § 76.1904.

Response to SageTV Comments

1. At page 8 of its *ex parte* submission, SageTV suggests that the gateway approach it favors will be "doomed for failure" if content output from the gateway device can be encrypted.[5] It points to the Commission's requirement in Rule 76.640(b), to make available DTCP to protect certain content over the mandated IEEE 1394 output of cable-supplied navigation devices, as an example of such a "doomed" approach. However, as the waiver petitions of Intel Corp., TiVo Inc., and Motorola Inc. have demonstrated, the failure of the 1394 interface to capture the home networking market's imagination had nothing to do with content protection generally or DTCP specifically.[6]

2. Contrary to the implications of the SageTV filing, DTCP is not to be automatically applied to all content available from the 1394 output.[7] In accordance with the Commission's encoding rules, unencrypted broadcast television is *never* to be encoded for encryption using DTCP (or any type of protection). Encryption is simply a non-issue for recording of such broadcast programming.[8] Moreover, neither DTLA nor the Commission's encoding rules determine whether protection is to be applied to content other than unencrypted broadcast television. That determination is made by the content provider. The Commission's (and DTLA's) encoding rules merely define the limits of protection that can be applied to particular types of content, if the content provider asserts that protection should be applied.

---

[5] Notably, other commenters that strongly favored a "gateway" approach did not cite the Commission's encoding rules and affiliated protection requirements as posing any impediment to their proposals.

[6] *See, In the Matter of Intel Corporation Petition for Waiver of 47 C.F.R. § 76.640(b)(4), Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices,* CS Docket No. 97-80, CSR-8229-Z, Petition for Waiver at 5-6, 13-14 (Oct. 7, 2009); *see also, In the Matter of Motorola Inc. Petition for Waiver of 47 C.F.R. § 76.640(b)(4), Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices,* CS Docket No. 97-80, Petition for Waiver at 4-6 (Nov. 25, 2009); *In the Matter of TiVo Inc. Petition for Waiver of 47 C.F.R. § 76.640(b)(4), Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices,* CS Docket No. 97-80, Petition for Waiver at 3-4, 7-9 (Nov. 6, 2009). DTLA has not submitted comments in any of these proceedings or in response to Public Notice #27.

[7] Because SageTV's comments refer only to the 1394 interface, DTLA likewise focuses its response with respect to how DTCP works over 1394. Notwithstanding, the operations and outcomes described in these comments are the same for all interface protocols to which DTCP has been mapped.

[8] 47 C.F.R. § 76.1904. *See* Plug and Play Order ¶¶ 50-54 ; As the Commission noted, at the time of their adoption there was no objection to the encoding rules as proposed for these defined business models. *Id.* ¶ 54.

3. With respect to content encoded for one generation of copies under the Commission's Rules, DTCP over 1394 will not impede consumers' ability to make the permitted protected copies.[9] For navigation devices with integrated recorders (such as PVRs), such recording generally occurs upstream, *i.e.*, before the 1394 output. In that circumstance, DTCP encryption has no effect on such recording because DTCP is applied only when the content exits the navigation device, not before it is recorded. For recording devices downstream, *i.e.*, external to the navigation device, a recorder with a DTCP-enabled 1394 port can receive and record copy one generation content output from the 1394 port of the navigation device.

4. SageTV's assertion, at 8, that DTCP does not allow recording on hard disk drives reflects a fundamental misunderstanding of DTLA's requirements.[10] DTLA's agreements specifically contemplate and facilitate recording on hard disk-based products, such as personal video recorders:

- The Compliance Rules for Sink Functions in the DTLA "Adopter Agreement," at pages B-7 to B-8, expressly contemplate use of a "bound recording" method, which would apply most appropriately to hard disk drive-based products. Specifically, Section 2.2.1.2 of those Compliance Rules provides that one generation of copies of DTCP-protected content can be made where:

  > The copy is stored using an encryption protocol that uniquely associates such copy with a single Licensed Product so that it cannot be played on another device or that no further usable copies may be made thereof . . . .[11]

- Notably, DTLA does not specify the encryption protocol to be used; only the characteristics of the protection that must be afforded. Any company can select and apply whatever technology, in its judgment, meets these requirements.

---

[9] To achieve the purpose of the Commission's Rules, any "first generation" recordings must be copied in a protected format that restricts making therefrom subsequent generations of copies.

[10] DTLA infers that SageTV misinterpreted the list of nine "Approvals for Persistent Storage and Digital Output Reprotection Technology" as defining the only storage methods permitted under the Adopter Agreement. (List available online at http://dtcp.com/data/DTLA%20Approved%20Technologies%20090901.pdf). As explained with respect to "bound recording" methods, this is incorrect. Even as to that list, however, one of the approved technologies, "Secure Architecture for Intelligent Attachment ("SAFIA") is designed for protection of audiovisual content (including content protected with DTCP) on removable hard disk drives. *See, e.g.*, http://www.cptwg.org/Assets/Presentations%202005/SAFIA_and_iVDR%2006022005CPTWG.pdf

[11] DTCP Adopter Agreement, available at http://dtcp.com/data/DTLA-AA-06302007.pdf

- Section 2.2.1.4 of the Compliance Rules (which essentially corresponds to Commission Rule 76.1904(2)) specifically refers to copying to a personal video recorder as a type of "bound recording medium."[12]

- Sections 2.2.3 and 2.2.4 explicitly refer to hard disk drive ("HDD") recording of copy one generation content in an integrated multi-recording device and for back-up purposes as a single logical copy.[13]

Therefore, DTCP does enable recordings to be made on hard disk-based recording products, and gives manufacturers substantial flexibility in how to do so.

In summary, DTLA submits there is no reason for the Commission to doubt that its encoding rules can continue to be effectuated, including with the use of DTCP and other encryption-based technologies, without impeding the growth of home networking and digital recording, and without discrimination against any particular recording medium.

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
1627 Eye Street NW
10th Floor
Washington, D.C. 20006
202.204.3514
sgreenstein@constantinecannon.com

---

12 *Id.* at B-7 ("Copy One Generation Decrypted DT Data that is copied in a personal video recorder or other bound recording medium pursuant to Section 2.2.1.2… .").

13 *Id.* at B-7 to B-8.