BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
Expanding Consumers' Video Navigation Choices	)	MB Docket No. 16-42
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80

REPLY COMMENTS OF
DIGITAL TRANSMISSION LICENSING ADMINISTRATOR, LLC

Digital Technology Licensing Administrator LLC ("DTLA"), the entity that licenses the Digital Transmission Content Protection technology ("DTCP"), appreciates this opportunity to respond to comments submitted to date in this rulemaking. In the DSTAC proceeding, and in the initial round of comments, current and potential DTCP Adopters have promoted their view of how DTCP will prove useful in an MVPD ecosystem conducive to innovative navigation products and distribution systems provided by third parties.[1] DTLA agrees that DTCP link protection can continue to play a valuable role in enabling interoperability of competitive retail devices on home networks. DTLA's participation in the DSTAC proceeding was limited to providing factual information in response to comments that inaccurately described past and current iterations of DTCP, and to informing the discussions with updated public information about ongoing improvements to the DTCP technology.

DTLA has reviewed comments in this proceeding that reference DTCP, and finds it necessary to submit reply comments to address certain misstatements and mischaracterizations about DTCP. Some of the comments critique the use of link protection generally, or observe that content protection technologies such as DTCP were not intended to solve every concern an

[1] *See, e.g.*, comments of the Telecommunications Industry Association, and the Consumer Video Choice Coalition.

MVPD might have.[2] Some comments suggest DTCP does not give content owners enough control over the protected network;[3] others, ironically, protest that content owners exert too much control over DTLA and DTCP.[4] Remaining commenters who admit they lack direct knowledge of DTCP's current implementations and future plans, nonetheless make suppositions critical of DTCP. DTLA recognizes that these comments reflect concerns that are tertiary to the fundamental reasons for their oppositions to the NPRM. DTLA nevertheless remains willing to work collaboratively with these and other stakeholders to enhance DTCP in a way that balances the interests of DTCP Adopters, MVPDs, and content owners, consistent with the pro-competitive and pro-consumer objectives embodied in the NPRM.

DTLA believes that DTCP has played, will continue to play, a useful role in content protection for content delivery and home networking. DTCP's primary benefits are robust technological and legal protection for content transmissions to, within, and from the home and personal network on reasonable and non-discriminatory terms, which are available to Adopters without individual negotiations with content owners. DTCP is implementable by large and smaller Adopters at a reasonable cost. Moreover, DTCP remains available to any content owner without license or fee. Therefore, DTLA submits this reply to explain the facts of the current and future attributes of DTCP, and its potential relevance to the competitive ecosystem envisioned by the NPRM.

---

[2] *See, e.g.*, Comments of Motion Picture Association of America at 25, and National Cable Television Association at 43 and NCTA Technical Report at 3 and 20, noting that DTCP does not address channel assignments, channel selection, protection of networks, or other functions unrelated to audiovisual content protection. Similarly, MPAA's assertion that DTCP does not address "password sharing" highlights a strength of DTCP—which does not rely on passwords for protection. DTCP authentication within the home and via mobile devices is based on a cryptographically secure use of device certificates embedded in the device, and is far more robust than password protection.

[3] Comments of MPAA at 24.

[4] *See* Comments of AT&T.

I. DTCP's Current Status and Role in Content Protection

DTLA's past submissions to the FCC explain generally the origins of DTCP, its licensing structure, and its role in content protection, which need not be repeated here.[5] In this section, DTLA addresses comments that have inaccurately described the current state of DTCP.

1. Like all content protection technologies, DTCP is not an open "standard."[6] All content protection relies on the combination of robust cryptographic algorithms and technology with legal enforceability. The latter requires use of proprietary intellectual property assets, so that the license can define the terms for compliance and the necessary levels of robustness for the ultimate benefit of copyright owners whose content is protected by DTCP. DTCP also incorporates confidential cryptographic elements and signed certificates issued by a private trusted key generation facility.

To the extent DTCP has become a *de facto* standard used by more than 160 licensees, DTLA attributes that interest in large measure to policy choices it made from the outset. First, unique among content protection technologies for a networked environment, DTCP is licensed on reasonable and nondiscriminatory terms. Second, DTLA designed DTCP to seamlessly interoperate securely with, rather than be walled off from, other vendors' content protection systems. Third, DTCP supports secure transmission of protected content for display and recording in a manner that accommodates reasonable and customary consumer behavior. Fourth, DTLA attempted to assure that its technological and legal requirements made DTCP readily implementable by its Adopters.

---

[5] *See* DTLA letters dated August 7, 2015 and October 8, 2015, http://apps.fcc.gov/ecfs/comment/view?id=60001097038, and http://apps.fcc.gov/ecfs/comment/view?id=60001302909.
[6] *See* NCTA comments at 98.

2. DTCP is a bidirectional content protection technology. Both the source of the content and the receiving (sink) device authenticate each other, and any "sink" can also include a "source" and vice versa. The limitation in some CableCARD contexts to one-way operation, observed by one commenter, and the resulting accusation that DTCP only defeats the threats to such devices "existing in the 1990s," results from contractual restrictions imposed by the DFAST license, not any technical constraint inherent in DTCP.[7] To the contrary, DTLA has regularly amended its Compliance Rules, Robustness Rules, and Specifications, in response to requests of its Adopters and Content Participants to update DTCP with additional capabilities and more robust protection.[8] Each update was subjected to prior review by DTLA's Content Participants. Without objection, each was deemed appropriate to meet then-current threat models. And, each was circulated to DTCP Adopters for comment in advance of final publication.

3. Some commenters assert, incorrectly, that DTCP is unable to accommodate new business models. DTLA created its content management information ("CMI") capability as a way to flexibly deliver usage and control information for new business models between devices and various content protection platforms in a format-agnostic and cryptographically-secure way. This feature, like all DTCP features, was vetted with its Adopters and its Content Participants before it was finalized in the DTCP specification to ensure that it was technologically sound and sufficient to meet their needs. DTLA before and since has offered to content owners, MVPD

---

[7] *See* MPAA comments at 24. Moreover, CableLabs asserts the right under the aegis of that license to approve any material changes to the DTCP technology for use in DFAST, even after the DTCP major studio Content Participants already have fully reviewed and accepted those changes. This assertion has resulted in the past in delaying the availability of DTCP-IP and later improvements to DFAST licensees.

[8] DTLA released four Adopter Agreement license revisions with updated compliance and/or robustness rules between December 2011 and June 2015.

representatives, and its Adopters the opportunity to work with DTLA to develop CMI that would implement specific new business models. DTLA remains open to working with all stakeholders so that new versions of DTCP meet their business requirements. It is unfair, in DTLA's view, to attribute decisions not to cooperate with DTLA to any deficiency in DTCP—particularly where such entities primarily oppose the NPRM for more fundamental competitive reasons.[9]

4. The NCTA technical report inaccurately asserts that no DTCP certificates have been revoked in the 17 years since DTLA has issued its certificates.[10] DTLA has issued System Renewability Messages ("SRMs") carrying information for periodic revocation of expired common device keys in accordance with the provisions of its Adopter Agreement. Those SRMs are available to DTLA's Content Participants, and to its Adopters upon request.

Any MVPD *could* deliver DTCP SRMs to client devices. DTLA registered its CP_System_ID specifically to facilitate DTCP SRM delivery over ATSC broadcast services in the United States (as well as DBS services in Europe).[11] However, DTLA is unaware of any domestic service provider that has implemented it.

In any event, *not* revoking a multitude of unique certificates is, in DTLA's view, a mark of DTCP's success. Over the last 17 years, DTLA has experienced no need to revoke unique keys based on improper conduct (such as theft or cloning of keys).[12]

---

[9] Similarly, contrary to AT&T's comments at 21, the elements of "DTCP+" – including CMI – have been available in the DTCP Specification and licenses to all DTCP Adopters since early 2011. At CableLabs's request, CableLabs reviewed and approved all in-scope elements of "DTCP+" under the CableLabs licenses.

[10] *Id.* at 21 n. 35.

[11] Europe's DVB Services provides the registration facility for identifiers for content protection system revocation lists. *See* http://www.dvbservices.com/identifiers/cp_system_id, link to System_ID allocation table.

[12] Similarly, DTLA is aware of no instance to date of hacking of DTCP, failure of robustness, or improper third party or other misconduct adverse to the integrity or protections offered by DTCP.

5. Commenters correctly note that DTCP-IP does not currently support common encryption.[13] Until this proceeding, no Content Participant or current or potential Adopter had requested it. As a matter of technology, DTCP-IP, DTCP-HE, or DTCP-2 can support common encryption. DTLA would be willing to enable it if there is sufficient interest from Content Participants or DTCP Adopters.

6. Finally, some commenters contend that link protection is riskier than any other type of content protection because it allegedly creates a "single point of attack." Whether protection is provided using a unitary DRM system or a series of technologically and contractually linked systems, the same content protection functions have to be provided, and hackers with professional tools and skills will search for the point of greatest vulnerability wherever it can be found. Strong linked protection systems are not inherently any more vulnerable than a DRM system of equivalent robustness. As DTLA has noted in the past, the current version of DTCP uses industry-strength standard cryptographic techniques that have proven robust in the field.

II. Continuing License and Development Work for DTCP: DTCP-2 and DTCP-HE

A. DTCP-2

DTLA has presented publicly to the Copy Protection Technical Working Group a detailed presentation describing a new version of DTCP to protect high value enhanced video content formats, such as Ultra High Definition and High Dynamic Range, against unauthorized interception, retransmission, or copying. DTLA filed a copy of that presentation with the FCC.[14] As DTLA previously has observed, the stronger cryptographic techniques embodied in "DTCP-

[13] AT&T comments at 47; NCTA comments at 128.
[14] *See* DTLA February 11, 2016 *ex parte* letter and presentation, at http://apps.fcc.gov/ecfs/comment/view?id=60001395226.

2" meet or exceed the MovieLabs recommendations for link protection,[15] and meet or exceed the robustness of HDCP 2.2 (which currently is approved by content owners and in commercial use for protection of Ultra HD 4k and HDR audiovisual content). Prior to that presentation, DTLA and its Content Participants concurred that these technological elements of DTCP-2 addressed their concerns. DTLA and its Content Participants also have reached general agreement on the robustness elements needed to protect such enhanced video content. The remaining provisions under discussion relate generally to enforcement, and additional time has been required to collaboratively address and avert the types of attacks recently experienced by content protection methods other than DTCP. DTLA and its Content Participants have been meeting regularly to finalize these requirements for DTCP-2, and DTLA remains optimistic that these discussions will conclude successfully in the near term.

The goal for DTLA remains, as it always has been, to provide a robust content protection solution that is readily implementable by multiple Adopters, in many countries around the world, who otherwise would not need contractual relationships with content owners to bring their products to market. DTLA appreciates that DirecTV was able, through its content license agreements with content owners, to reach agreement on interim robustness additions to DTCP-IP, and DTLA raised no objection to their efforts. However, the interim solutions they implement are not suitable for all DTCP Adopters, for several reasons. First, the RVU requirements pertain to only one of the many potential applications of DTCP, and to only one source of DTCP-protected content. DTLA needs to accommodate the requirements of its other Adopters who offer different types of devices and applications. Second, DirecTV can impose subscriber-level

[15] MovieLabs Specification for Enhanced Content Protection Version 1.1 (Feb. 2015), http://movielabs.org/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%20v1.1.pdf

controls that are not pertinent to DTCP per se, but that nevertheless satisfy content owner concerns by limiting unauthorized access to the network.[16] Third, compliance with the language of the MovieLabs recommendations may be acceptable where augmented by other, more definite, contractual obligations to content owners. However, that generalized language is not suitable for implementation in DTCP Robustness Rules. Phrases like "secure media pipeline," "secure execution environment," "chain of trust," lack the requisite specificity and commonality of interpretation to be reliably implementable by a broad range of large and small DTCP Adopters from many countries and speaking many languages; and any resulting ambiguity could prove counterproductive to the goals of robust protection. Finally, the technical attributes of DTCP-2 include both more flexible features for content owners and Adopters, and a higher level of robustness, than has been permitted on an interim basis for DirecTV.

For about one year MVPDs in the RVU Alliance have been able through this accommodation to use DTCP-IP to deliver Ultra HD services. DTLA hopes that this marketplace advantage over other DTCP Adopters will be short-lived. In keeping with DTLA licensing policies and the overall purpose of the rulemaking, DTLA is working to finalize its work with its Content Participants so that all Adopters soon can benefit from DTCP-2. In the meantime, DTLA appreciates the support of the other Adopters who advocate the use of DTCP-IP and DTCP-2 in the final rule.

[16] For example, DirecTV DTLA also notes that at least one of the "security elements" accepted by DirecTV—a "whitelist of authenticated client devices authorized by content licensors" (Dulac Declaration at 5-6)—could be used to perpetuate a "walled garden" environment that excludes third party competitive navigation devices. A benefit of DTCP is that it provides such a broad authorization, without requiring each manufacturer to obtain licenses from each individual network or content licensor.

B. DTCP-HE

DTLA previously noted in submissions to the Commission that in recent years DTLA had worked with a contributor and the Content Participants to enable use of DTCP from a commercial head-end or server to the home.[17] The perceived benefit of the proposal, similar to the goal of this proceeding, was to facilitate communications from an external server directly to display and recording devices connected to the external network, without need of a "set-top box." DTLA anticipates that DTCP-HE could use DTCP-IP, DTCP-IP (with the same types of robustness applied by DirecTV), or DTCP-2, depending upon Adopter requirements.

Conclusion

DTLA appreciates the interest of commenters in the potential role of DTCP in supporting a competitive market for navigation devices, and welcomes this opportunity to submit these reply comments. Should the Commission have any questions, or if it believes that any updated submissions would be useful, DTLA would be pleased to respond.

Respectfully submitted,

/s/ Stephen P. Balogh
Stephen P. Balogh
DTLA President

/s/ Michael Andre
Michael Andre
DTLA TWG Chair

/s/ Seth D. Greenstein
Seth D. Greenstein
DTLA Policy Chair
sgreenstein@constantinecannon.com
(202) 204-3514

May 23, 2016

[17] In response to the comments of DirecTV concerning its lack of awareness of DTCP-HE, DTLA and its Content Participants maintained the DTCP-HE development project as confidential, inasmuch as the contributor and its initial anticipated customers would have been competitors to DirecTV and other MVPDs. Notwithstanding, DTLA remains open to working with DirecTV or any other MVPD or Adopter to meet their technology and business needs through DTCP-HE as well as DTCP-2 and any future iterations of DTCP.