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

In the Matter of:	)	
	)	
Digital Output Protection Technology and Recording Method Certifications	)	
	)	
MagicGate Type-R for Secure Video Recording for Hi-MD Hardware	)	MB Docket No. 04-55
	)	
MagicGate Type-R for Secure Video Recording for Memory Stick PRO Software	)	MB Docket No. 04-56
	)	
MagicGate Type-R for Secure Video Recording for Hi-MD Software	)	MB Docket No. 04-57
	)	
MagicGate Type-R for Secure Video Recording for Memory Stick PRO Hardware	)	MB Docket No. 04-58
	)	
SmartRight	)	MB Docket No. 04-59
	)	
Vidi Recordable DVD Protection System	)	MB Docket No. 04-60
	)	
High Bandwidth Digital Content Protection	)	MB Docket No. 04-61
	)	
Content Protection Recordable Media for Video Content	)	MB Docket No. 04-62
	)	
TiVoGuard Digital Output Protection Technology	)	MB Docket No. 04-63
	)	
Digital Transmission Content Protection	)	MB Docket No. 04-64
	)	
Helix DRM Trusted Recorder	)	MB Docket No. 04-65
	)	
Windows Media Digital Rights Management Technology	)	MB Docket No. 04-66
	)	
D-VHS	)	MB Docket No. 04-68
	)	

ORDER

Adopted: August 4, 2004 **Released: August 12, 2004**

By the Commission: Commissioner Martin approving in part, concurring in part and issuing a statement.

TABLE OF CONTENTS

Paragraph Number

I. INTRODUCTION 1

II. OVERVIEW OF THE CONTENT PROTECTION TECHNOLOGIES AND RECORDING METHODS 5

A. Output Protection Technologies 5
1. Digital Transmission Content Protection 5
2. High Bandwidth Digital Content Protection 14
3. TiVoGuard Digital Output Protection Technology 19
B. Recording Methods 24
1. Content Protection Recordable Media for Video Content 24
2. Vidi Recordable DVD Protection System 30
3. MagicGate Type-R for Secure Video Recording 35
4. D-VHS 41
C. Digital Rights Management Technologies 47
1. Windows Media Digital Rights Management Technology 47
2. Helix DRM Trusted Recorder 53
3. SmartRight 57

III. DISCUSSION 61

A. Scope of Approval 62
B. Scope of Redistribution Control 69
1. Localization 69
2. Copy Restrictions 75
C. Technical Matters 78
D. License Terms 79
1. Approval of Downstream Technologies and Interoperability 81
2. Licensing of Intellectual Property 84
3. Content Provider Third Party Beneficiary and Enforcement Rights 92
4. Change Management 94
5. Revocation and Renewal 100
6. Compliance and Robustness 104
7. Associated Obligations 105

IV. ORDERING CLAUSES 108

I. INTRODUCTION

1. As a part of its efforts to further the digital television ("DTV") transition, on November 4, 2003, the Commission issued a *Report and Order and Further Notice of Proposed Rulemaking* adopting a redistribution control content protection system to protect against the mass indiscriminate

redistribution of digital broadcast television ("*Broadcast Flag Order*").[1] In conjunction with this system, the Commission set forth in Section 73.9008 of its rules an interim process by which digital output protection technologies and recording methods could be authorized for use in Covered Demodulator Products required to respond and give effect to the Redistribution Control Descriptor set forth in ATSC Standard A/65B (the "ATSC flag" or "flag").[2] Proponents of specific digital output protection technologies and recording methods can certify to the Commission under this interim process that their technology is appropriate for use with Unscreened Content and Marked Content to give effect to the flag.[3]

2. The above-captioned thirteen certifications were received in response to a January 23, 2004, public notice issued by the Commission opening an initial certification window.[4] Each certifying entity submits that its technology is appropriate for use in DTV reception equipment to give effect to the flag.[5] In response, various parties filed responses and oppositions with respect to the certifications during the requisite comment and opposition window.[6] Each certifying entity subsequently filed a reply.

3. Section 73.9008(d) of the Commission's rules sets forth the relevant criteria that the Commission may consider, where applicable, in evaluating the appropriateness of digital output

[1] *Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003).

[2] *Broadcast Flag Order,* 18 FCC Rcd at 23574-76; 47 C.F.R. § 73.9008. *See* ATSC A/65B, Program and System Information Protocol for Terrestrial Broadcast and Cable (ATSC 2003). Covered Demodulator Product is defined in Section 73.9000(f) of the Commission's rules and, for the purposes of this *Order*, includes Peripheral TSP Products, as defined in Section 73.9000(j) of the Commission's rules. 47 C.F.R. §§ 73.9000(f), (j). Section 73.9000(g) defines a demodulator as a component, or set of components, that is designed to perform the function of 8-VSB, 16-VSB, 64-QAM or 256-QAM demodulation and thereby produce a data stream for the purpose of digital television reception. *Id*. § 73.9000(g).

[3] *Broadcast Flag Order,* 18 FCC Rcd at 23575; 47 C.F.R. § 73.9008. Unscreened Content is specifically defined in Section 73.9000(q) of the Commission's rules, but in simple terms means digital broadcast television content that has not been screened for the flag. 47 C.F.R. § 73.9000(q). Likewise, Marked Content is defined in Section 73.9000(l) of the Commission's rules and refers to digital broadcast television content that is marked with the flag. *Id*. § 73.9000(l).

[4] *See Initial Certification Window*, DA No. 04-145 (rel. Jan. 23, 2004).

[5] *See* Certification for MagicGate Type-R for Secure Video Recording for Hi-MD Hardware as an Authorized Recording Technology ("MagicGate Hi-MD Hardware Certification"); Certification for MagicGate Type-R for Secure Video Recording for Memory Stick Pro Software as an Authorized Recording Technology ("MagicGate Memory Stick Pro Software Certification"); Certification for MagicGate Type-R for Secure Video Recording for Hi-MD Software as an Authorized Recording Technology ("MagicGate Hi-MD Software Certification"); Certification for MagicGate Type-R for Secure Video Recording for Memory Stick Pro Hardware as an Authorized Recording Technology ("MagicGate Memory Stick Pro Hardware Certification"); SmartRight Certification for FCC Approval for Use With the Broadcast Flag ("SmartRight Certification"); Vidi Recordable DVD Protection System Broadcast Flag Certification ("Vidi Certification"); Certification of Digital Content Protection, LLC for Approval of its High Bandwidth Digital Content Protection as an Approved Digital Output Protection Technology ("HDCP Certification"); Certification of 4C Entity, LLC for Approval of its Content Protection Recordable Media for Video Content as an Approved Digital Content Protection Recording Method ("CPRM Certification"); Broadcast Flag Certification of TiVo Inc. ("TiVoGuard Certification"); Certification of Digital Transmission Licensing Administrator LLC for Approval of DTCP as an Authorized Output Protection Technology ("DTCP Certification"); Broadcast Flag Certification Response to the Federal Communications Commission of RealNetworks, Inc. ("Helix Certification"); Certification of Windows Media Digital Rights Management Technology for Use with Broadcast Flag ("WMDRM Certification"); Certification of Victor Company of Japan, Limited for Approval of its "D-VHS" Format as a Digital Content Protection Technology and Recording Method to be Used in Covered Demodulator Products ("D-VHS Certification").

[6] *See Certifications for Digital Output Protection Technologies and Recording Methods to be Used in Covered Demodulator Products*, DA No. 04-715 (rel. Mar. 17, 2004).

protection technologies and recording methods under this interim process.[7] These criteria include:

> (1) Technological factors including but not limited to the level of security, scope of redistribution, authentication, upgradability, renewability, interoperability, and the ability of the digital output protection technology to revoke compromised devices;
>
> (2) The applicable licensing terms, including compliance and robustness rules, change provisions, approval procedures for downstream transmission and recording methods, and the relevant license fees;
>
> (3) The extent to which the digital output protection technology or recording method accommodates consumers' use and enjoyment of unencrypted digital terrestrial broadcast content; and
>
> (4) Any other relevant factors the Commission determines warrant consideration.[8]

4. Based upon the records in the above-captioned proceedings, we conclude that all thirteen digital output protection technologies and recording methods satisfactorily fulfill these evaluative criteria, subject to the conditions described herein. We believe each technology will provide content owners with reasonable assurance that digital broadcast television content will not be indiscriminately redistributed while protecting consumers' use and enjoyment of broadcast video programming and facilitating innovative consumer uses.[9] This, in turn, will ensure the continued availability of high value digital television content to consumers through broadcast outlets.[10] We reiterate that our goal of preventing the indiscriminate redistribution of digital broadcast television content "will not (1) interfere with or preclude consumers from copying broadcast programming and using or redistributing it within the home or similar personal environment as consistent with copyright law, or (2) foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution."[11] Below we provide an overview of each proposed technology, and then consider in a consolidated fashion various issues implicated in multiple certifications.

II. OVERVIEW OF THE CONTENT PROTECTION TECHNOLOGIES AND RECORDING METHODS

A. OUTPUT PROTECTION TECHNOLOGIES

1. Digital Transmission Content Protection

5. Digital Transmission Content Protection ("DTCP") is a digital output protection technology that employs a cryptographic protocol to protect various types of "audio/video entertainment content from unauthorized copying, interception and tampering as it traverses high performance digital

[7] 47 C.F.R. § 73.9008(d).

[8] *Id*. § 73.9008(d). In this context, unencrypted digital terrestrial broadcast content is defined as "audiovisual content contained in the signal broadcast by a digital television station without encrypting or otherwise making the content available through a technical means of conditional access, and includes such content when retransmitted in unencrypted digital form." *Id*. § 73.9000(p).

[9] *Broadcast Flag Order,* 18 FCC Rcd at 23552.

[10] *Id.* at 23554-55.

[11] *Id.* at 23555.

interfaces."[12] The DTCP specification was jointly created by Hitachi, Ltd., Intel Corporation, Matsushita Electrical Industrial, Co., Ltd., Sony Corporation, and Toshiba Corporation (the "5C Companies") but is licensed directly from the Digital Transmission Licensing Administrator, LLC ("DTLA").[13] Although DTCP was originally designed to transport compressed video over IEEE 1394, it has since been mapped[14] to other physical connectors such as USB, Op-iLink, and MOST, as well as to Internet Protocol ("IP") for use with wired and wireless transports, including Ethernet and 802.11.[15]

6. DTLA asserts that the availability of DTCP over many protocols and platforms promotes flexibility, convenience and consumer choice, and emphasizes that DTCP is already incorporated into numerous DTV products.[16] DTLA further avers that DTCP is an authorized digital output protection technology under the Dynamic Feedback Arrangement Scrambling Technique ("DFAST") and POD-Host Interface License agreements ("PHILA"), which are administered by representatives of the cable television industry.[17] DTCP has also been approved for the protection of movie content on DVDs by the DVD Copy Control Association ("DVD CCA") and authorized as an approved transport protection method for use with Content Protection Recordable Media ("CPRM"), Content Protection for Prerecorded Media ("CPPM") and D-VHS.[18] DTLA indicates that it has signed 85 agreements with adopters, resellers and content participants and that Motion Picture Association of America, Inc. ("MPAA") member companies have expressed support for the use of DTCP in a broadcast flag regime.[19]

7. DTCP uses authentication, key exchange techniques, and content encryption as part of its protection system.[20] Under this system, a connected device must first verify through the exchange of keys that another connected device is "authentic," meaning also DTCP-compliant, before sharing protected information.[21] Content can receive varying levels of protection in the DTCP regime, which is communicated through the use of Copy Control Information ("CCI") embedded in the content stream.[22] DTLA explains that Marked Content will be encoded as "encryption plus nonassertion" ("EPN"), which triggers encryption as the content is transported, but permits unlimited copying in protected forms.[23] Unmarked digital terrestrial broadcast transmissions will be able to be both copied and redistributed freely

[12] DTCP Certification at 1.

[13] *Id*. at 1-2.

[14] Mapping refers to the process by which the parameters of a content protection technology are defined for use in connection with a specific transport or media.

[15] DTCP Certification at 3. DTLA also recently completed work on mapping DTCP to Bluetooth. *Id*.; *see* Letter from Seth Greenstein, McDermott, Will and Emory, to Marlene Dortch, FCC at Attachment (June 24, 2004) ("*DTLA 6/24/04 Ex Parte*").

[16] DTCP Certification at 13-14, 25-26.

[17] *Id*. at 13.

[18] *Id*. at 15.

[19] DTLA Reply at 42; DTCP Certification at 14.

[20] When it encrypts content, DTCP uses 56 bit M6 encryption in connection with physical transports and 128 bit AES encryption over IP. DTCP Certification at 5-6.

[21] *Id*. at 3-5. Authentication can be performed at a full or restricted level, depending on the type of content and devices involved. *Id*. at 4.

[22] *Id*. at 6-8. An Encryption Mode Indicator ("EMI") is a more readily-accessible indicator of CCI that is used to convey the appropriate encryption mode to sink devices. *Id*. at 7-8.

[23] *Id*. at 6-7.

without triggering authentication or encryption.[24]

8. The scope of redistribution for EPN-encoded content is limited as a result of the encryption of the content. A single content source can distribute the same protected content to 34 DTCP-compliant devices.[25] As a further restriction, DTLA states that it will not approve for use with DTCP any downstream output or recording technology that enables unauthorized redistribution outside home and personal networks.[26] The inherent length limitations of IEEE 1394 and USB serve this goal in the case of physical connectors.[27] With respect to network-based technologies using IP, DTLA commits to the localization of content through a limit of 3 on the Time to Live ("TTL") field in IP packets, which represents the number of routers through which an IP packet can pass before it is discarded.[28] Pursuant to its recently-completed localization work plan for DTCP over IP, DTLA has additionally committed to a limit of 7 milliseconds or less on Round Trip Time ("RTT"), which represents the amount of time that an IP packet and associated responses can travel between devices.[29] DTLA also affirms that it will use Wired Equivalency Privacy ("WEP") or Wi-Fi Protected Access ("WPA") encryption for the exchange of data over wireless IP transports.[30] Other localization mechanisms are being explored pursuant to a two-phase work plan.[31]

9. DTLA certifies that DTCP offers a high level of protection "designed to be effective to thwart or frustrate attempts to send DTCP-protected content to noncompliant devices, and to limit distribution of such protected content to DTCP-compliant devices within the home and personal network."[32] To ensure the integrity of its system, DTCP utilizes System Renewability Messages ("SRMs") as the basis for revocation where a device is no longer authorized to receive content.[33] SRMs, which contain a list of revoked device certificates, are generated by DTLA and delivered through content and new devices.[34] Upon receipt of an SRM identifying a particular device as revoked, that device is rendered unable to exchange content with other devices via DTCP.[35] Since it believes revocation is a

[24] *Id*. at 6.

[25] *Id*. at 10.

[26] *Id*.

[27] *Id*. Likewise, MOST is used to interconnect audiovisual devices in automobiles or a "similarly contained mobile environment," thereby restricting the scope of redistribution. *Id*.

[28] *Id*. at 10-11.

[29] Letter from Brad Hunt, MPAA, and Seth Greenstein, McDermott, Will & Emery, to Kenneth Ferree, FCC at 2 (July 20, 2004) ("*DTLA 7/20/04 Ex Parte*"); Letter from Seth Greenstein, McDermott, Will & Emery, to Marlene Dortch, FCC (July 22, 2004) ("*DTLA 7/22/04 Ex Parte*").

[30] DTCP Certification at 10-11.

[31] *Id*. at 11; DTLA Reply at 3; Letter from Seth Greenstein, McDermott, Will & Emery, to Marlene Dortch, FCC at Attachment (June 1, 2004) ("*DTLA 6/1/04 Ex Parte*"); *DTLA 7/20/04 Ex Parte* at 1-2 (noting that although its localization work plan is complete with respect to DTCP-IP, "[w]ork … continues as to the localization of additional protocols to which DTCP has been mapped, including IEEE 1394 and 1394-similar transports, USB, Bluetooth and MOST")..

[32] DTCP Certification at 11.

[33] *Id*. at 8-9. Revocation involves the process of disabling a key so that it can be no longer used for decryption. Depending on the system architecture of a particular technology, revocation can therefore be applied to specific applications or content, individual devices, or a class of devices. This process is distinguished from renewal, which we interpret as the ability of a content protection technology to change its cryptography without hardware or software upgrades.

[34] *Id*.

[35] *Id*.

drastic measure, DTLA has identified a limited number of circumstances in which it may be invoked.[36]

10. Licensing of DTCP is accomplished through two primary documents – an adopter agreement and a content participant agreement.[37] The DTCP adopter agreement grants manufacturers a license for any intellectual property rights that are "necessary" to implement the DTCP specification, and requires in return that adopters agree not to assert any patent claims that they might possess that fall within the same "necessary claims" scope.[38] DTLA suggests that this necessary claims and reciprocal non-assert approach to intellectual property licensing is commonly used in licenses for digital video content protection technologies.[39]

11. The DTCP adopter agreement also sets forth the compliance and robustness rules governing source and sink function devices; DTLA characterizes these rules as mirroring those in the DFAST license.[40] Change management is provided for with respect to the compliance rules and the DTCP technical specification.[41] DTLA describes its change management rights as limited to non-material changes.[42] Under this process, content participants receive advance notice and the right to object to certain proposed amendments to the DTCP specification, adopter and content participants agreements.[43] Adopters who participate in a Content Protection Implementers Forum receive advance notice and have the opportunity to comment on proposed changes to the compliance rules.[44] Content participants also possess third party beneficiary rights to enforce equitable and injunctive relief against adopters who violate the DTCP adopter agreement's compliance and robustness rules.[45]

12. DTLA submits that DTCP was designed to coexist and be compatible with existing and

[36] Revocation may only be imposed where: (a) a Device Key and corresponding Device Certificate have been cloned such that the same key and certificate are found in more than one device or product; (b) a Device Key and/or Device Certificate have been lost, stolen, intercepted, misdirected or made public or disclosed; or (c) revocation is required by court order or other government authority. *Id*. at 9, n.1; *see also id*. at Appendix 2 at § 4.2 ("*DTCP Adopter Agreement*").

[37] *See DTCP Adopter Agreement*; *see also* DTCP Certification at Appendix 3 ("*DTCP Content Participant Agreement*").

[38] DTCP Certification at 16; *DTCP Adopter Agreement* at §§ 5.3-5.4. DTLA has indicated that it will not enforce its intellectual property rights in DTCP against content owners that use or require use of DTCP without signing the *DTCP Content Participant Agreement*, so long as the content owner follows the applicable encoding rules. DTCP Certification at 12, Appendix 4.

[39] DTCP Certification at 16.

[40] *Id*. at 19.

[41] *Id*. at 20-22; *DTCP Adopter Agreement* at § 3.3.

[42] Although DTLA indicates that material changes to the DTCP specification are not allowed, it reserves the right to make limited changes to enable DTCP to be used over additional interfaces, to correct omissions or errors, or to make changes that would clarify, but not materially amend, alter or expand the specification. DTCP Certification at 20; *DTCP Adopter Agreement* at § 3.3.1. Any mandatory changes to the DTCP specification must be implemented within 18 months after adoption by DTLA. DTCP Certification at 21; *DTCP Adopter Agreement* at § 3.3. Under the terms of the *DTCP Adopter Agreement*, DTLA cannot make any changes to the compliance rules that would materially increase the cost or complexity of implementation of products "except as DTLA, in consultation with [content] owners … may conclude is necessary to ensure and maintain content protection." *DTCP Adopter Agreement* at § 3.3.3. Changes to the compliance rules become effective within 12 months of adoption by DTLA. DTCP Certification at 21; *DTCP Adopter Agreement* at § 3.3.

[43] *DTCP Content Participant Agreement* at § 3.7.

[44] DTCP Certification at 21; *DTCP Adopter Agreement* at § 3.4.

[45] DTCP Certification at 12; *DTCP Content Participant Agreement* at §§ 3.4, 11.2, Ex. A.

future content protection technologies.[46] Notwithstanding this fact, DTLA considers it essential that DTCP only pass protected content to downstream technologies that provide protection at least as effective as DTCP.[47] In evaluating downstream output protection technologies and recording methods, DTLA considers a number of criteria, including the applicable compliance and robustness rules, enforcement provisions, and content owner and adopter support.[48] Any resulting decision to approve a technology is subject to change management review by content participants.[49] DTLA represents that it has not refused a request for approval from any technology proponent and has to date approved High Bandwidth Digital Content Protection ("HDCP"), D-VHS and CPRM.[50]

13. DTLA asserts that the DTCP adopter and content participant agreements have always been freely offered on a nondiscriminatory basis to any potential signatory.[51] Both content participants and adopters pay annual administration fees, with an additional per certificate fee for adopters.[52] DTLA provides that these fees were established on a cost-recovery basis and have not increased since 1999 for adopters and 2001 for content participants.[53]

2. High Bandwidth Digital Content Protection

14. HDCP is a digital output protection technology designed by Intel Corporation to protect uncompressed digital video content from a consumer source device to a consumer display device.[54] HDCP is licensed by Digital Content Protection, LLC ("DCP") for use with the Digital Visual Interface ("DVI") and the High Definition Multimedia Interface ("HDMI").[55] DCP indicates that HDCP enjoys support from all MPAA members and has been approved by the DVD CCA and under the DFAST, DTCP, CPRM, and D-VHS licenses.[56] To date, 85 product manufacturers have signed an HDCP license and compliant products are currently available in the marketplace.[57] Although HDCP does not permit content to be copied, DCP suggests that this will not inhibit consumer use and enjoyment of digital broadcast television content since HDCP is used at points in the consumer environment where they are viewing and hearing content rather than enabling a networked application or making a copy of content.[58]

15. HDCP uses explicit authentication between source and display devices, in combination

[46] DTCP Certification at 2.

[47] *Id*. at 22-23.

[48] *Id*. at 22, Appendix 5.

[49] *Id*. at 23; *DTCP Content Participant Agreement* at § 3.7.

[50] DTCP Certification at 23. An approval request filed by Philips Electronics North America Corporation ("Philips") and Hewlett-Packard Company ("Hewlett-Packard") for their Vidi Recordable DVD Protection System ("Vidi") is currently under consideration by DTLA. DTLA Reply at 48, n.66.

[51] DTCP Certification at 18.

[52] *Id*. at 24. Content participants pay an annual administration fee of $18,000, while adopters' administration fees range from $10,000 to $18,000 per year. *Id*. Per certificate fees range from $ 0.05 to $0.07. *Id*.

[53] *Id*. at 24-25.

[54] HDCP Certification at 3.

[55] *Id*.

[56] *Id*. at 8-9.

[57] *Id*. at 9.

[58] *Id*. at 10.

with content encryption, to prevent the unauthorized interception of content.[59] Since HDCP was designed to be the "last link" in the consumer chain in which other technologies permit authorized copying or management of content in networked environments, HDCP was not designed to accommodate different CCI states and instead contains a uniform prohibition on copies.[60] Display devices may not output decrypted content in any form, unless the display device is serving as a repeater to another display device and the content is output digitally and re-encrypted with HDCP.[61] As a practical matter, these restrictions effectively truncate the scope of redistribution for content protected with HDCP and prevent its interoperability with downstream content protection technologies. Revocation is accomplished in the HDCP universe much the same as it is with DTCP – in a narrow set of prescribed circumstances and through the transmission of revocation lists in SRMs, which are delivered in media and transmitted content.[62]

16. The HDCP licensing regime is comprised of four types of agreements, including an adopter and a content participant license.[63] Manufacturers that execute the HDCP adopter agreement receive a "a nonexclusive worldwide license to Intel-owned necessary claims and to Intel and DCP owned trade secrets and copyrights with respect to HDCP and the HDCP specification."[64] As a companion to its necessary claims approach to intellectual property licensing, the HDCP adopter agreement contains a reciprocal non-assert similar to that in the DTCP adopter agreement.[65]

17. DCP describes the HDCP compliance rules as simple, given the technology's limited purpose, but recognizes that the robustness rules follow the detailed ones employed by DTCP, CPRM and DFAST.[66] DCP explains that it can make changes to the HDCP specification, compliance and robustness rules, and procedural appendix, but only where changes that implicate product design do not interfere with the backward compatibility of HDCP or do not materially increase the cost or complexity of implementation of the HDCP specification.[67] Pursuant to these change management procedures, content

[59] Each device contains an array of 40 secret device keys, each 56-bit in length, which are used for authentication. *Id*. at 7. A 84-bit block cipher is used to encrypt data. *Id*. at 4.

[60] *Id*. at 3, 5; Letter from Bruce Turnbull, Weil, Gotshall & Manges, to Marlene Dortch, FCC at 1-3 (June 25, 2004) ("*DCP 6/25/04 Ex Parte*").

[61] HDCP Certification at 3, Appendix 2 at Exhibit C, § 5.3 ("*HDCP Adopter Agreement*").

[62] HDCP Certification at 8. The legal standard for revocation also mirrors DTCP in that it may only be imposed where: (a) a Device Key Set associated with a Key Selection Vector have been cloned and found in more than one device; (b) a Device Key Set associated with a Key Selection Vector have been lost, stolen, intercepted, misdirected or made public or disclosed; or (c) revocation is required by court order or other government authority. *Id*.; *see also HDCP Adopter Agreement* at § 7.2.

[63] HDCP Certification at 12. The other agreements cover component manufacturers and resellers. *Id*. Since many of the relevant provisions of the component manufacturer and reseller agreements are largely duplicated in the adopter agreement, we focus our description of the HDCP licensing regime on its adopter and content participant agreements.

[64] *Id*.; *HDCP Adopter Agreement* at § 2.1.

[65] HDCP Certification at 13; *HDCP Adopter Agreement* at § 2.2. A similar reciprocal non-assert is contained in the HDCP content participant agreement. *See* HDCP Certification at 13, Appendix 5 at § 2.2 ("*HDCP Content Participant Agreement*").

[66] HDCP Certification at 5; *HDCP Adopter Agreement* at Ex. C, D. The HDCP compliance rules prohibit HDCP from being used to copy and/or redistribute content, except in limited cases to another digital display over a repeater. HDCP Certification at 5.

[67] HDCP Certification at 14; *HDCP Adopter Agreement* at § 5.1. All changes require advance notice, with 12 to 18 months before effectiveness for changes implicating product design. HDCP Certification at 14; *HDCP Adopter Agreement* at § 5.2; *HDCP Content Participant Agreement* at § 3.6(b).

participants have the right to review and object to any changes that are material and adverse to the integrity or security of HDCP, the operation of HDCP with respect to the protection of content from unauthorized output, transmission, interception or copying, or content participant rights under the HDCP content participant agreement.[68] Content participants also gain third party beneficiary rights to seek injunctive relief against implementations that materially fail to satisfy any HDCP adopter agreement requirements, as well as rights to initiate and participate in the revocation process.[69]

18. DCP does not articulate the basis on which its license is offered to potential signatories, but details the applicable license fees, including annual administrative fees for adopters and content participants, as well as unit fees to cover the costs of generating and delivering keys.[70] DCP submits that these fees do not reflect full market rates, but are aimed at cost recovery.[71]

3. TiVoGuard Digital Output Protection Technology

19. TiVo Inc. ("TiVo") has certified its TiVoGuard digital output protection technology ("TiVoGuard") as a component in its end-to-end security system that allows content to be transferred among a limited number of TiVo devices registered with a TiVo customer account, also known as a "secure viewing group."[72] TiVo states that it does not offer TiVoGuard as a free-standing digital output protection or recording technology, and has no intention to do so in the future.[73] In place of publicly licensing TiVoGuard, TiVo contractually obligates equipment manufacturers that produce TiVo digital video recorders ("DVRs"), and other devices for which TiVo specifies the hardware and software, to utilize TiVoGuard as a part of its security specifications.[74] TiVo indicates that these equipment manufacturers may, at their discretion, also include in their final product other digital output protection technologies that have been approved by the Commission.[75] MPAA, on behalf of its content owner members, does not support TiVo's certification.[76]

20. TiVo explains that TiVoGuard limits the redistribution of protected content to a secure viewing group of devices that belong to the same owner and that are associated with the same TiVo

[68] HDCP Certification at 14; *HDCP Content Participant Agreement* at §§ 3.5-3.6(b).

[69] HDCP Certification at 12; *HDCP Content Participant Agreement* at § 3, Ex. B; *HDCP Adopter Agreement* at § 11.6, Ex. A, § 2.

[70] DCP questions the Commission's ability to review the license terms applicable to content protection technologies and recording methods. HDCP Certification at 10, n.2. Adopters pay an administrative fee of $15,000 per year, with unit fees ranging from $1,000 to $5,000 based on the number of key sets involved. *Id*. at 15; *HDCP Adopter Agreement* at Ex. A, § 1. The applicable administrative fee for content participants is $50,000 per year. HDCP Certification at 15; *HDCP Content Participant Agreement* at Ex. C.

[71] HDCP Certification at 11, 15. The change management provision governing license fees limits adjustments to costs. *Id*. at 14; *HDCP Adopter Agreement* at § 4.2; *HDCP Content Participant Agreement* at § 4.1.

[72] TiVoGuard Certification at 25.

[73] *Id*. at 34.

[74] *Id*. at 32-33. TiVo indicates that it has granted licenses to several manufacturers to create products providing DVR capabilities, including Pioneer Corporation, Toshiba Corporation, Toshiba American Consumer Products, Inc., Sony Electronics, Inc., Humax Corporation, Ltd. and DIRECTV, Inc. *Id*. at 32. TiVo specifies that it has not yet licensed its TiVoToGo technology to any equipment manufacturer. *Id*. TiVo avers that it will contractually require downstream product manufacturers to design and build devices in accordance with the Commission's flag compliance and robustness rules. TiVo Reply at 3-4.

[75] TiVoGuard Certification at 33.

[76] Opposition to the Application of TiVo for Interim Authorization of TiVoGuard by the Motion Picture Association of America, Inc., *et al*. at 3 ("MPAA Opposition to TiVo"). *See infra* ¶¶ 70, 92, 94, 101, 104.

service account, which must in turn be billed to the owner's credit card.[77] Under its current policy, TiVo limits the number of devices comprising a secure viewing group to 10, but makes provision for waivers in exceptional circumstances.[78] A single TiVo device can be in only one secure viewing group and must be registered through a password protected web interface or by calling TiVo customer support.[79] TiVo uses Transmission Control Protocol/Internet Protocol ("TCP/IP") as a communications channel between networked devices to transfer encrypted content.[80]

21. Before transmitting encrypted content to another device, TiVoGuard authenticates the intended recipient device to ensure it is in the same secure viewing group and that it periodically communicates with TiVo's central servers.[81] TiVo asserts that the ability of its devices to regularly communicate with its central servers plays an important role not only in authentication but also in revocation, renewal and upgrade.[82] When a TiVo device contacts the central servers, it receives a "TiVoGuard certificate" which authorizes the device up to a specific expiration date.[83] If a TiVo device does not contact the central server to routinely update its TiVoGuard certificate, the device is automatically revoked and can no longer send content to another device.[84] TiVo indicates that revocation information can also be transmitted to a device or class of devices during their regular communications with the central server to affirmatively revoke their authorizations.[85] In a similar manner, TiVo submits that it can send secure software and data updates from its central servers to upgrade and renew its TiVoGuard technology.[86]

22. Once a recipient TiVo device has been authenticated, TiVoGuard permits content to be transferred to that device in encrypted form.[87] TiVo states that its encryption protocols use unique keys to encrypt small blocks of content to limit the amount of content potentially compromised if a cryptographic attack were successful.[88] Upon receipt by the downstream TiVo device, the content is re-encrypted in a

[77] TiVoGuard Certification at 25-26; Letter from James Burger, Dow, Lohnes & Albertson, PLLC, to Susan Mort, FCC at Attachment (June 22, 2004) ("*TiVo 6/22/04 Ex Parte*"); Letter from James Burger, Dow, Lohnes & Albertson, PLLC, to Marlene Dortch, FCC at Attachment (July 21, 2004) ("*TiVo 7/21/04 Ex Parte*").

[78] TiVoGuard Certification at 25. TiVo's user agreement expressly limits subscribers to transfer content among 10 DVRs on a single account, but TiVo will consider waiver requests initiated by subscribers up to an absolute cap of one-tenth of one percent of TiVo subscribers. Letter from James Burger, Dow, Lohnes & Albertson, PLLC, to Marlene Dortch, FCC at Attachment (July 28, 2004) ("*TiVo 7/28/04 Ex Parte*"). Written waiver requests must indicate: (1) why a waiver is necessary, (2) where the devices will be located, (3) that the subscriber reaffirms the provisions in the TiVo user agreement requiring the subscriber not to violate copyright laws and pledging to only use copyrighted content for personal, non-commercial purposes. *Id*. TiVo indicates that it will exercise care and consistency in granting waivers. *Id*. Waivers may be granted for up to 20 devices, although the current technical limit is 16. *Id*.; TiVoGuard Certification at 25.

[79] TiVoGuard Certification at 25-26.

[80] *Id*. at 26-27; *TiVo 6/22/04 Ex Parte* at 1.

[81] *TiVo 6/22/04 Ex Parte* at 3. Authentication is accomplished using a 894-bit El Gamal public and private key pair. TiVoGuard Certification at 17.

[82] TiVoGuard Certification at 26.

[83] *Id*.

[84] *Id*. at 26, 32.

[85] *Id*. at 26, 31-32.

[86] *Id*. at 31.

[87] *TiVo 6/22/04 Ex Parte* at 5.

[88] TiVo specifies that it uses a 128-bit Linear-Feedback Shift Register stream cipher to encrypt content in small blocks of between 5 and 15 minutes length. TiVoGuard Certification at 16, 27-30; *TiVo 6/22/04 Ex Parte* at 4-6. (continued....)

manner that uniquely associates it with that device and prevents it from being accessed in usable form by another product, except by TiVoGuard or another Commission-approved output protection technology.[89]

23. TiVo submits that TiVoGuard is also designed to function with a new implementation known as TiVoToGo, which allows a TiVo customer to transfer recorded content from a TiVo DVR in their secure viewing group to a personal computer equipped with TiVo Media Player software and a hardware plug-in dongle also registered to the customer's account.[90] Since a registered dongle must be physically connected to a computer for a consumer to be able to view transferred content, only one computer at a time can be used in association with a specific dongle.[91] Once a consumer inserts the dongle into a computer and initiates a request to view protected content stored on a DVR registered to their account, the TiVo Media Player software authenticates the request by verifying that the content is protected with TiVoGuard and is authorized to be played in connection with that specific dongle.[92] The protected content is sent through the Internet to the TiVo Media Player which authenticates it and uses the dongle to decrypt it for display on the computer.[93] TiVo asserts that this proprietary combination of hardware and software protects content in accordance with the Commission's rules.[94]

B. RECORDING METHODS

1. Content Protection Recordable Media for Video Content

24. CPRM is an encryption-based recording method that can be used to record standard definition ("SD") and limited resolution digital video content to removable or portable media including DVD-R/-RW, SD Memory Cards, Secure CompactFlash and Microdrive media.[95] CPRM was developed by International Business Machines Corporation, Intel Corporation, Matsushita Electric Industrial Co., Ltd., and Toshiba Corporation (the "4C Companies") and is licensed by 4C Entity, LLC ("4C").[96] 4C states that CPRM has widespread support among MPAA members and the more than 100 product manufacturers that have taken a license to produce compliant devices.[97] In addition, CPRM has been approved by DTLA under the DTCP downstream approval procedures, and authorized by Japan's BS Digital Broadcast Promotion Association as a secure recording method for use with content distributed through Japan's digital satellite and terrestrial television broadcast system.[98] 4C promotes CPRM as

(...continued from previous page)
As a part of this process, a 128-bit Blowfish cipher is used for symmetric data exchange. TiVoGuard Certification at 16, 27-29.

[89] TiVoGuard Certification at 28; *TiVo 6/22/04 Ex Parte* at 5.

[90] TiVo Reply at 18.

[91] *Id*.

[92] *Id*. at Attachment at 4.

[93] *Id*. at Attachment at 4-5.

[94] *Id*. at Attachment at 1. For example, TiVo argues that TiVoToGo complies with 47 C.F.R. § 73.9000(r) in that unencrypted media travels in a direct path from the memory of the TiVo Media Player to the user's display via a protected bus. *Id*.

[95] CPRM Certification at 3. Although CPRM can be used to record both audiovisual and pure audio content, it has only been certified to the Commission for its audiovisual implementation. *Id*. at 3, n.1. As such, references in this *Order* to CPRM only refer to its audiovisual implementation. DVD-R/-RW is an optical disc media format supported by technologies companies such as Pioneer, Toshiba and Apple.

[96] *Id*. at 3.

[97] *Id*. at 11.

[98] *Id*.

beneficial to consumers in that it affords flexibility in the playback of content on any CPRM-compliant player, including computer-based products and more traditional consumer electronics devices.[99]

25. CPRM employs a publicly-scrutinized encryption algorithm to cryptographically bind content to the recordable media.[100] As a result, protected content can only be read on CPRM-compliant devices.[101] Although the binding process prevents serial copies from being made directly from an individual piece of media, CPRM-compliant devices have the ability to respond to and assert DTCP's CCI encoding, including EPN for Marked Content, so as to allow unlimited, multiple secure copies of content to be made.[102] 4C adds that the scope of redistribution is further restricted through a requirement that compliant devices only permit the digital output of content through DTCP or HDCP protected connectors.[103]

26. 4C describes two forms of revocation and upgrade applicable to CPRM-compliant devices.[104] In its standard implementation where each compliant device has its own unique key, revocation can be achieved on a device-by-device basis through the dissemination of a list of revoked device keys in new media.[105] When a device attempts to playback content on media identifying its device key as revoked, it will be unable to decrypt that content.[106] 4C specifies that revocation may only occur in a limited number of circumstances.[107] In implementations of CPRM where a series of devices share the same key, an upgrade system that changes the keys on a regular interval is required.[108]

27. CPRM is licensed through a series of adopter and reseller agreements, in addition to a content participant agreement.[109] The adopter agreement applicable to audiovisual content grants a limited license to use the CPRM technology to protect digital content in accordance with the applicable compliance rules, and takes a necessary claims and reciprocal non-assert approach to the licensing of patent claims.[110] 4C identifies two sets of compliance rules for recorders and players, each of which

[99] *Id*. at 12.

[100] *Id*. at 5. A 56-bit C2 Block Cipher is used to encrypt content. *Id*.

[101] *Id*. When a consumer seeks to playback encrypted content, a form of implicit authentication occurs between the CPRM-compliant device and the recorded media. *Id*. at 9.

[102] *Id*. at 6-7; *see also* CPRM Certification at Appendix 1 at Ex. C-3a, § 4.2 ("*CPRM Adopter Agreement*").

[103] CPRM Certification at 7-8; *CPRM Adopter Agreement* at Ex. C-3a, § 4.1.1.

[104] CPRM Certification at 9-10.

[105] *Id*. at 10. The list of revoked device keys are contained in the Media Key Block in newly made media. *Id*.

[106] *Id*.

[107] The legal standard for revocation, which echoes those of DTCP and HDCP, is triggered where: (a) a Device Key Set has been cloned and found in more than one device (other than legitimate key sharing between limited numbers of devices and software); (b) a Device Key Set has been lost, stolen, intercepted, misdirected or made public or disclosed; or (c) revocation is required by court order or other government authority. *Id*.; *see also CPRM Adopter Agreement* at § 9.2.

[108] CPRM Certification at 10.

[109] *Id*. at 6, 14, 17. A single adopter agreement covers both audiovisual content and prerecorded audio content, while separate agreements apply to parties that make related components and to manufacturers of SD memory cards for storing content. *Id*. Since many of the relevant provisions of the component manufacturer, media manufacturer and reseller agreements are largely duplicated in the primary adopter agreement, we focus our description of the CPRM licensing regime on its primary adopter and content participant agreements.

[110] *Id*. at 4, 8, 14; *CPRM Adopter Agreement* at § 1.4.1, 2.2-2.4, 2.7; *see also* CPRM Certification at Appendix 3, § 3 ("*CPRM Content Participant Agreement*").

articulates how protected content is to be handled, including limits on digital output of protected content to DTCP or HDCP protected connectors.[111] The corresponding robustness rules prescribe a high level of protection.[112]

28. Under the adopter agreement's change management terms, provision is made for 4C to make non-material changes to the CPRM technical specifications once they are released at version 1.0, and to make changes in the compliance rules that are necessary to protect content.[113] Although adopters that serve on the 4C Advisory Board and content participants can each request changes to the CPRM adopter agreement, its compliance rules, or the technical specifications, only content participants have the right to object to changes that are material and adverse to their interests.[114] Content participants also have third party beneficiary rights to take direct enforcement actions against adopters whose products are materially non-compliant with the CPRM adopter agreement's compliance and robustness rules.[115]

29. 4C indicates that it offers its licenses to potential adopters on reasonable and non-discriminatory terms and stresses that it views the licensing of content protection technologies to be market-enabling.[116] As such, 4C states that its license fees are aimed at actual costs rather than commercial rates.[117] Fee adjustments are limited to any increase in 4C's administrative costs.[118]

2. Vidi Recordable DVD Protection System

30. Vidi Recordable DVD Protection System ("Vidi") also utilizes encryption to record and bind SD video content to compliant DVD+R/+RW media.[119] Vidi has been jointly developed by Philips Electronics North America Corp. ("Philips") and Hewlett-Packard Company ("Hewlett-Packard") and will be directly licensed by Philips.[120] Although Vidi is a new technology that has yet to be deployed in the marketplace, Philips and Hewlett Packard indicate they have the endorsement of industrial partners including Ricoh Company, Ltd., Yamaha Corporation, and Ahead Software AG.[121] Subject to certain caveats raised in its response to the certification filed by Philips and Hewlett-Packard which are addressed

[111] CPRM Certification at 7; *CPRM Adopter Agreement* at Ex. C-3a, §§ 3.3, 4.

[112] The robustness rules require that the security functions cannot be defeated or circumvented using widely available tools or specialized tools and can only with difficulty be defeated using professional tools. *CPRM Adopter Agreement* at Ex. C-4, § 4.

[113] CPRM Certification at 16; *CPRM Adopter Agreement* at § 3.3. Non-material changes to the compliance rules require 90 days advance notice, while all other changes to the compliance rules or specifications require 18 months notice prior to implementation. *Id*.

[114] CPRM Certification at 17; *CPRM Adopter Agreement* at § 3.2; *CPRM Content Participant Agreement* at § 2.2, 3.7.

[115] CPRM Certification at 17; *CPRM Adopter Agreement* at § 8.5-8.10; *CPRM Content Participant Agreement* at § 2.4, 8.

[116] CPRM Certification at 12-13.

[117] *Id*. at 13, 16-17. Adopters pay annual administrative fees ranging from $6,000 to $12,000 with per unit fees, where applicable, ranging from $ 0.02 to $ 0.14. *Id*.; *see also CPRM Adopter Agreement* at § 4, Ex. B. Content participants pay an undisclosed annual administration fee. *CPRM Content Participant Agreement* at § 4.

[118] CPRM Certification at 17; *CPRM Adopter Agreement* at § 4.1-4.2; *CPRM Content Participant Agreement* at § 4.

[119] Vidi Certification at 6. DVD+R/+RW is an optical disc media format developed by the DVD+RW Alliance, which includes Philips, Hewlett Packard, Dell and other technology companies.

[120] *Id*. at 1; *see also id*.at Appendix B ("*Vidi Content Protection Agreement*").

[121] Vidi Certification at 1.

below, MPAA supports the approval of Vidi for use in this context.[122] Philips and Hewlett Packard promote Vidi as a technology that "fully embraces consumer use and enjoyment of digital television content."[123]

31. As with CPRM, the Vidi recording process binds content to the physical media using proven cryptographic methods.[124] Vidi DVDs must be used to record or play protected content, which will only be accessible on Vidi-compliant drives and software applications.[125] Vidi will read and record Marked Content as having the "Redistribution Controlled" CCI state, which allows the content to be copied freely, but prohibits its indiscriminate redistribution.[126] The binding of content to physical media prevents serial copies from being directly made from that piece of media, but usable copies can be made with a Vidi-compliant device.[127] To restrict the scope of redistribution, Vidi-compliant devices will only output digital forms of protected content using Commission-approved output protection technologies.[128]

32. Should the security of a Vidi-compliant device be compromised, individual devices can be revoked in specific circumstances.[129] Revocation is accomplished through the inclusion of a list of revoked device keys in Vidi DVDs.[130] At the time a consumer initiates the recording or playback of content, an authentication process will verify whether that device appears on the revocation list contained in the Vidi DVD.[131] If so, authentication will fail and the device will be unable to utilize that media.[132] As new media is released, Philips and Hewlett Packard anticipate that compromised devices will quickly be rendered obsolete.[133]

33. Philips offers a single Vidi license to all adopters and content participants.[134] Under the terms of the license, Philips and Hewlett-Packard agree not to assert the intellectual property they each have in Vidi within the relevant "field of use," which includes the use of Vidi to protect content in this

[122] MPAA Response to Philips and Hewlett Packard at 2.

[123] Vidi Certification at 2.

[124] *Id*. at 7, 13-14. A 128-bit AES cipher is used in the encryption process. *Id*.

[125] *Id*. at 7. Philips and Hewlett-Packard emphasize that Vidi DVDs will still be compatible with legacy equipment to make unprotected recordings in order to preserve the use of existing consumer equipment to the greatest extent possible. *Id*. at 7, 29.

[126] *Id*. at 16.

[127] *Id*. at 7, 17.

[128] *Id*. at 10.

[129] *Id*. at 9. Hardware keys may be revoked if: (1) the same key is found in more than one device, (2) the implementer has disclosed the key, or (3) the key has been lost, stolen or otherwise misdirected. *Id*. at 25; *Vidi Content Protection Agreement* at Art. 7, Ex. D. Software keys may be revoked if: (1) the key is found in applications widely used in conjunction with unauthorized copying or distribution, (2) the key has been lost, stolen or otherwise misdirected or is made public, or (3) if the software key is used in a hardware device. Vidi Certification at 25; *Vidi Content Protection Agreement* at Art. 7, Ex. D.

[130] Vidi Certification at 9.

[131] *Id*. As part of the recording and playback process, Vidi authenticates the device through the use of device ids and node key sets to access root keys contained in the device key blocks on Vidi DVDs. *Id*. at 7-8.

[132] *Id*. at 9.

[133] *Id*.

[134] *Id*. at 23.

context.[135] Adopters and content participants must in turn covenant to license any patent claims necessary for the use of Vidi on reasonable and nondiscriminatory terms.[136] Philips and Hewlett-Packard liken this approach to intellectual property licensing to that used in the DFAST license.[137] The Vidi license also contains compliance rules that are modeled after those established by the Commission for Covered Demodulator Products.[138] As noted by Philips and Hewlett-Packard, Vidi's robustness rules reflect a higher standard than that imposed by the Commission since Vidi will also be used to protect copy controlled content.[139]

34. Change management is accomplished under what Philips and Hewlett-Packard characterize as an open process.[140] Limited changes to the Vidi technical specification and the compliance and robustness rules are permitted, with advance notice and an opportunity to comment provided to adopters and content participants.[141] Objections are handled through consultation and arbitration.[142] Third party beneficiary rights are granted to content participants to seek injunctive relief and liquidated damages for material breaches likely to compromise the security of content protected by Vidi or of the underlying technology itself.[143] Philips and Hewlett-Packard assert that Vidi will be offered to all potential signatories on reasonable, non-discriminatory, and equal terms and conditions.[144] Implementers must pay a one-time fee at execution of the Vidi license, in addition to a per device key fee, while content participants are responsible for annual administrative fees.[145]

3. MagicGate Type-R for Secure Video Recording

35. Sony Corporation ("Sony") has certified four derivations of its MagicGate Type-R for Secure Video Recording ("MagicGate") technology, including hardware and software implementations for each of two different media formats - Hi-MD recordable discs and Memory Stick PRO.[146] Sony states that while it will license its hardware implementations to third parties, it intends to keep its software

[135] *Id*. The relevant field of use is defined as the use of Vidi to encrypt audiovisual content on DVD+R and DVD+RW discs, to decrypt such content for playback from such discs, and the embedding of keys in blank discs. *Id*.; *Vidi Content Protection Agreement* at §§ 1.2, 2.1.

[136] Vidi Certification at 22-23; *Vidi Content Protection Agreement* at § 2.5.

[137] Vidi Certification at 22-23.

[138] *Id*. at 22; *Vidi Content Protection Agreement* at Ex. A, § A.1.2.2.1; *see also* 47 C.F.R. §§ 73.9003-73.9006.

[139] Vidi Certification at 22; *Vidi Content Protection Agreement* at Ex. A; *see also* 47 C.F.R. §§ 73.9007.

[140] Vidi Certification at 24-25.

[141] Examples of permitted changes include those needed to fix errors, omissions or bugs, to add analog outputs, and to conform to government mandates. *Id*.; *Vidi Content Protection Agreement* at §§ 6.2, 6.3.1-6.3.2.

[142] Vidi Certification at 25; *Vidi Content Protection Agreement* at §§ 6.2, 6.3.3-6.3.5.

[143] Vidi Certification at 3, 22, 25, 29; *Vidi Content Protection Agreement* at Art. 9. In order to seek injunctive relief, content participants must produce audiovisual content with an annual turnover threshold of € 100,000,000. Vidi Certification at 25; *Vidi Content Protection Agreement* at § 1.2, 9.3.2.

[144] Vidi Certification at 3, 22, 27, 29; *Vidi Content Protection Agreement* at § 13.9.

[145] The one-time implementer fee is € 5,000, with a per device key fee of € 0.05. Vidi Certification at 23-24; *Vidi Content Protection Agreement* at § 3.1a, 3.3.1. Content participants pay an annual fee of € 10,000. Vidi Certification at 24; *Vidi Content Protection Agreement* at § 3.1b.

[146] *See* MagicGate Hi-MD Hardware Certification; MagicGate Memory Stick PRO Software Certification; MagicGate Hi-MD Software Certification; MagicGate Memory Stick PRO Hardware Certification. Hi-MD recordable discs currently are available in either 300 MB or 1GB capacities. *See* Sony Reply at 5.

implementations proprietary for its own use and that of its affiliates.[147] Given the commonalities among these four implementations, we discuss them here in a consolidated fashion. Sony indicates that Fox, Warner Brothers and Sony Pictures Entertainment have deemed the security elements of this new technology as sufficient to protect against the unauthorized redistribution of content.[148] Sony also advances MagicGate from a consumer perspective, noting that the small format of its Hi-MD and Memory Stick PRO media promotes portability.[149]

36. MagicGate allows high definition ("HD"), SD or constrained resolution content to be transferred from a compliant device to a Secure Drive Module where the content is recorded and bound in encrypted format to either Hi-MD or Memory Stick PRO media.[150] Content recorded using MagicGate can be played back on any compliant MagicGate device using the same media format.[151] Since content is cryptographically bound in the recording process, it prevents usable bit-by-bit copies from being made directly from that media.[152] Marked Content will be treated as having DTCP's EPN encoding, thereby limiting its redistribution without any copy controls.[153] Sony currently restricts the digital output of MagicGate protected content to connectors using DTCP or HDCP.[154]

37. Revocation can be effectuated for individual devices in MagicGate hardware implementations and for all copies of a specific version of software in its software implementations.[155] Sony explains that revocation information can be propagated through the release of new media carrying

[147] MagicGate Hi-MD Hardware Certification at 2; MagicGate Memory Stick PRO Software Certification at 2; MagicGate Hi-MD Software Certification at 2; MagicGate Memory Stick PRO Hardware Certification at 2.

[148] Sony acknowledges that Fox, Warner Brothers and Sony Pictures Entertainment have reserved final approval pending review of the MagicGate license terms. MagicGate Hi-MD Hardware Certification at 10-11; MagicGate Memory Stick PRO Software Certification at 10; MagicGate Hi-MD Software Certification at 10-11; MagicGate Memory Stick PRO Hardware Certification at 10-11.

[149] MagicGate Hi-MD Hardware Certification at 19; MagicGate Memory Stick PRO Software Certification at 14-15; MagicGate Hi-MD Software Certification at 15; MagicGate Memory Stick PRO Hardware Certification at 18-19.

[150] Content is transferred from a MagicGate compliant device to a Secure Drive Module over a Secure Authenticated Channel. MagicGate Hi-MD Hardware Certification at 3; MagicGate Memory Stick PRO Software Certification at 3; MagicGate Hi-MD Software Certification at 3; MagicGate Memory Stick PRO Hardware Certification at 3. USB is used in the transfer process. MagicGate Hi-MD Hardware Certification at 3; MagicGate Hi-MD Software Certification at 3; MagicGate Memory Stick PRO Software Certification at Appendix A at 8; MagicGate Memory Stick PRO Hardware Certification at Appendix A at 8.

[151] MagicGate Hi-MD Hardware Certification at 8; MagicGate Memory Stick PRO Software Certification at 8; MagicGate Hi-MD Software Certification at 8; MagicGate Memory Stick PRO Hardware Certification at 8.

[152] An Integrity Check Value is calculated using an AES-based hash. MagicGate Hi-MD Hardware Certification at 3, 6-7; MagicGate Memory Stick PRO Software Certification at 3, 6-7; MagicGate Hi-MD Software Certification at 3, 6-7; MagicGate Memory Stick PRO Hardware Certification at 3, 6-7. AES 128-bit encryption is used for both unscreened and marked content. *Id*.

[153] MagicGate Hi-MD Hardware Certification at 5; MagicGate Memory Stick PRO Software Certification at 5; MagicGate Hi-MD Software Certification at 5-6; MagicGate Memory Stick PRO Hardware Certification at 5.

[154] A limited exception is also made for computer products produced prior to June 30, 2005 that send a constrained image to DVI outputs. MagicGate Hi-MD Hardware Certification at 8, 15-16; MagicGate Memory Stick PRO Software Certification at 8, 11; MagicGate Hi-MD Software Certification at 8-9, 12; MagicGate Memory Stick PRO Hardware Certification at 8, 15.

[155] MagicGate Hi-MD Hardware Certification at 7; MagicGate Memory Stick PRO Software Certification at 7; MagicGate Hi-MD Software Certification at 7; MagicGate Memory Stick PRO Hardware Certification at 7.

updated lists of revoked devices and software.[156] If a MagicGate device or software implementation has been revoked, it will be unable to retrieve a common key that is necessary for decrypting content when it attempts authentication prior to recording or playback.[157]

38. MagicGate hardware implementations are licensed through a series of adopter agreements for device hardware, media, and integrated chip manufacturers, format agreements for the underlying Hi-MD and Memory Stick PRO formats, and content participant agreements.[158] The device hardware adopter agreements authorize manufacturers to implement MagicGate in conjunction with Hi-MD and Memory Stick PRO products and utilize a necessary claims and reciprocal non-assert approach to intellectual property licensing.[159] The applicable compliance rules detail the permitted output and recording controls applicable to Marked and Unscreened content.[160] Sony asserts that the robustness rules were modeled after those used in the DFAST license and are at least as protective of DTV content as the Commission's flag robustness requirements.[161] Although Sony will not be publicly licensing its software implementations, it pledges to maintain them by the same compliance and robustness requirements applicable to its hardware implementations.[162]

39. The device hardware adopter agreements provide for change management with respect to the MagicGate technical specifications and compliance and robustness rules in specific circumstances.[163]

---

[156] The revocation information consists of a list of revoked Device Node Keys for both hardware and software which is contained in the Enabling Key Block of new media. MagicGate Hi-MD Hardware Certification at 7-8; MagicGate Memory Stick PRO Software Certification at 7-8; MagicGate Hi-MD Software Certification at 7-8; MagicGate Memory Stick PRO Hardware Certification at 7-8.

[157] MagicGate Hi-MD Hardware Certification at 7; MagicGate Memory Stick PRO Software Certification at 7; MagicGate Hi-MD Software Certification at 7; MagicGate Memory Stick PRO Hardware Certification at 7.

[158] MagicGate Hi-MD Hardware Certification at 11-12; MagicGate Memory Stick PRO Hardware Certification at 11. In the case of the Hi-MD Hardware implementation, the device hardware adopter agreement is also supplemented with a Video Addendum. MagicGate Hi-MD Hardware Certification at 11; *see also* MagicGate Hi-MD Hardware Certification at Appendix E ("*Hi-MD Video Addendum*"). Since many of the relevant provisions of the media manufacturer, integrated chip manufacturer, and format agreements are largely duplicated in the device hardware adopter agreement, we focus our description of the MagicGate licensing regime on its device hardware adopter and content participant agreements.

[159] MagicGate Hi-MD Hardware Certification at 11-12; MagicGate Memory Stick PRO Hardware Certification at 11-12; *see also* MagicGate Hi-MD Hardware Certification at Appendix D, Art. II ("*Hi-MD Device Hardware Adopter Agreement*"); MagicGate Memory Stick PRO Hardware Certification at Appendix D, Art. II ("*Memory Stick PRO Device Hardware Adopter Agreement*").

[160] MagicGate Hi-MD Hardware Certification at 15-16; MagicGate Memory Stick PRO Hardware Certification at 14-16.

[161] MagicGate Hi-MD Hardware Certification at 16-17; MagicGate Memory Stick PRO Hardware Certification at 16.

[162] MagicGate Memory Stick PRO Software Certification at 2, 11-13; MagicGate Hi-MD Software Certification at 2, 11-13.

[163] The change management provisions in the *Hi-MD Device Hardware Adopter Agreement* and *Memory Stick PRO Device Hardware Adopter Agreement* prohibit any revisions to the MagicGate technical specifications, compliance or robustness rules that would materially increase the cost or complexity of implementation of devices, or that would require material modifications to product design or manufacturing of devices, unless changes are necessary to protect content. MagicGate Hi-MD Hardware Certification at 17; MagicGate Memory Stick PRO Software Certification at 13; MagicGate Hi-MD Software Certification at 13-14; MagicGate Memory Stick PRO Hardware Certification at 16-17; *Hi-MD Device Hardware Adopter Agreement* at Art. III; *Memory Stick PRO Device Hardware Adopter Agreement* at Art. III. Upon notification of any changes, adopters must comply within 18 months. *Id*.

Content participants receive advance notice of proposed changes and may object where a change will have a material and adverse effect on their interests.[164] Content participants may also assert third party beneficiary rights over adopters with respect to the compliance and robustness rules.[165] As a counterpoint, Sony notes that adopters possess their own third party beneficiary rights over content participants with respect to content encoding rules.[166]

40. Like DTLA, Sony considers it essential that all MagicGuard implementations only pass protected content to downstream technologies that provide protection at least as effective as MagicGate.[167] Sony does not detail the procedures or standards applicable to the approval process, but specifies that future decisions to approve downstream technologies are subject to change management review by content participants.[168] To date, Sony has approved DTCP and HDCP.[169] Finally, Sony indicates that it will offer all adopter agreements on a nondiscriminatory basis.[170] All adopters and content participants pay a one-time license fee.[171] Device hardware adopters pay an additional per unit key fee.[172]

4. D-VHS

[164] Specifically, content participants may object where a proposed change will have a material and adverse effect on the integrity and security of MagicGate, the operation of MagicGate with respect to the protection of content from unauthorized transmission, interception, or copying, or the rights of content participants with respect to MagicGate. MagicGate Hi-MD Hardware Certification at 17-18; MagicGate Memory Stick PRO Hardware Certification at 17; *see also* MagicGate Hi-MD Hardware Certification at Appendix C, §§ 3.5-3.6 ("*Hi-MD Content Participant Agreement*"); MagicGate Memory Stick PRO Hardware Certification at Appendix C, §§ 3.5-3.6 ("*Memory Stick PRO Content Participant Agreement*").

[165] MagicGate Hi-MD Hardware Certification at 13-14; MagicGate Memory Stick PRO Software Certification at 10-11; MagicGate Hi-MD Software Certification at 11; MagicGate Memory Stick PRO Hardware Certification at 13-14; *Hi-MD Content Participant Agreement* at §§ 3.3, 12.1, Ex. A; *Hi-MD Video Addendum* at Art. VI; *Memory Stick PRO Content Participant Agreement* at §§ 3.3, 12.1, Ex. A.

[166] MagicGate Hi-MD Hardware Certification at 14; MagicGate Memory Stick PRO Hardware Certification at 13-14; *Hi-MD Content Participant Agreement* at § 11.2; *Hi-MD Device Hardware Adopter Agreement* at Art. X, Ex. B; *Memory Stick PRO Content Participant Agreement* at § 11.2; *Memory Stick PRO Device Hardware Adopter Agreement* at Art. X, Ex. B.

[167] MagicGate Hi-MD Hardware Certification at 18; MagicGate Memory Stick PRO Software Certification at 13-14; MagicGate Hi-MD Software Certification at 14-15; MagicGate Memory Stick PRO Hardware Certification at 17-18.

[168] MagicGate Hi-MD Hardware Certification at 18; MagicGate Memory Stick PRO Software Certification at 13-14; MagicGate Hi-MD Software Certification at 14-15; MagicGate Memory Stick PRO Hardware Certification at 17-18.

[169] MagicGate Hi-MD Hardware Certification at 8, 15-16; MagicGate Memory Stick PRO Software Certification at 8; MagicGate Hi-MD Software Certification at 8-9, 12; MagicGate Memory Stick PRO Hardware Certification at 8.

[170] MagicGate Hi-MD Hardware Certification at 12; MagicGate Memory Stick PRO Hardware Certification at 12.

[171] For both the Hi-MD and Memory Stick PRO hardware implementations, the one time fees are: (1) device hardware adopters, ¥ 300,000, (2) content participants, $ 12,000. MagicGate Hi-MD Hardware Certification at 15; *Hi-MD Device Hardware Adopter Agreement* at Ex. I; *Hi-MD Content Participant Agreement* at Ex. B; MagicGate Memory Stick PRO Hardware Certification at 14; *Memory Stick PRO Device Hardware Adopter Agreement* at Ex. I; *Memory Stick PRO Content Participant Agreement* at Ex. B.

[172] The Device Node Key fee applicable to Hi-MD device hardware adopters is ¥ 2 per key. MagicGate Hi-MD Hardware Certification at 15; *Hi-MD Video Addendum* at Ex. H. For Memory Stick PRO device hardware adopters, the applicable fee is ¥ 3 per key. MagicGate Memory Stick PRO Hardware Certification at 14; *Memory Stick PRO Device Hardware Adopter Agreement* at Ex. H.

41. D-VHS is a recording format developed and licensed by Victor Company of Japan, Limited ("JVC") for use with removable magnetic tape cassettes to record SD or HD video content.[173] JVC states that D-VHS is fully backward-compatible and can record and play back analog video content on VHS or S-VHS cassettes.[174] As such, JVC suggests that D-VHS is user friendly and familiar to consumers.[175] JVC promotes industry adoption of D-VHS in so far as several manufacturers produce compliant products and Twentieth Century Fox, Universal, Artisan and DreamWorks studios have agreed to release prerecorded HD movies in D-VHS format.[176] D-VHS has also been provisionally approved as a secure storage technology by DTLA for DTCP-protected content.[177]

42. D-VHS operates in a fundamentally different manner than CPRM, Vidi and MagicGate. JVC explains that, as a format rather than an added content protection technology, D-VHS uses a proprietary variant-seed method to scramble content as part of the recording process.[178] D-VHS cassettes will therefore only play on devices that utilize JVC's proprietary format specifications.[179] According to JVC, the fact that D-VHS does not employ means for revocation, renewal or upgrade is also attributable to its nature as a format-related consumer electronics device.[180] In order to restrict the scope of redistribution, JVC limits the digital output of protected content to connectors utilizing DTCP or HDCP.[181] If a multi-industry consensus on the security of additional downstream protection technologies emerges, JVC is committed under the terms of its content beneficiary agreement to permit their use in D-VHS products.[182]

43. Another key difference distinguishing D-VHS from its counterparts involves the marking of content during the recording process. Specifically, Marked Content will be signaled as "copy restricted" in Copy Generation Management System ("CGMS") when recorded in order to effectuate redistribution control.[183] Despite this copy restriction, JVC provides that format-cognizant D-VHS products capable of recognizing EPN encoding can make additional copies from the original recording.[184] A recent change to the D-VHS copy protection requirements facilitates the ability of format non-cognizant devices to read the embedded CCI and EPN indicator in content and convert it to a "copy one generation" setting when output to DTCP.[185] This change in essence permits a consumer to link two D-

[173] D-VHS Certification at 3.

[174] *Id*.

[175] *Id*. at 11.

[176] *Id*. at 9-10. Manufacturers producing D-VHS products include Panasonic, Mitsubishi, Hitachi, Sony, Toshiba and Marantz. *Id*. at 10.

[177] *Id*. at 9-10.

[178] *Id*. at 7.

[179] This in effect results in an implicit form of authentication. *Id*. at 8.

[180] *Id*.

[181] *Id*. at 5.

[182] *See Id*. at Appendix F, Art. 1(A) ("*Content Beneficiary Agreement*"). JVC offers a second content beneficiary agreement which has limited applicability to content owners releasing prerecorded HD content using JVC's D-Theater platform. D-VHS Certification at 11.

[183] D-VHS Certification at 11.

[184] *Id*. at 6, 11; *see also* Letter from Bruce Turnbull, Weil, Gotshal & Manges, LLP, to Marlene Dortch, FCC at 1-2 (June 24, 2004) ("*JVC 6/24/2004 Ex Parte*").

[185] *JVC 6/24/2004 Ex Parte* at 2.

VHS products and make multiple protected copies of Marked Content.[186]

44. In addition to offering a content beneficiary agreement, JVC licenses D-VHS through a format license applicable to manufacturers.[187] JVC specifies that it is the owner of, or has the right to sublicense, the patents necessary to implement the D-VHS specification for the manufacture of compliant products.[188] The format license requires adopters to abide by the terms of JVC's copy protection requirements, which have been supplemented to encompass redistribution control over digital broadcast television content.[189] Adopters must design and manufacture D-VHS products so as to effectively frustrate the alteration or circumvention of the copy protection requirements.[190] JVC undertakes pre-release testing of all D-VHS models to ensure their compliance with the copy protection requirements and JVC's robustness standards.[191]

45. Change management of the copy protection requirements is provided for in the content beneficiary agreement.[192] Specifically, content beneficiaries receive advance notice and an opportunity to object to any proposed changes in the copy protection requirements to reduce the level of content protection.[193] Third party beneficiary rights are also granted to content beneficiaries to take enforcement action against manufacturers of non-compliant D-VHS products.[194]

46. JVC states that licenses to manufacturers are available on reasonable and non-discriminatory terms, with certain provisos relevant to the D-VHS format.[195] Since D-VHS is a follow-on format to the original VHS format, JVC only permits VHS format licensees to accede to the D-VHS format license.[196] Although it generally offers the D-VHS format to any interested VHS licensee, JVC reserves the right to refuse to license D-VHS to any entity that has not met its obligations with respect to format compliance, content protection requirements, or fee payment.[197] Further, JVC determines pricing on a licensee-by-licensee basis, based in large part on the nature and extent of each licensee's patents that are granted back to JVC.[198] JVC stresses that its terms and fees have been accepted in the marketplace without any objection from licensees or prospective licensees.[199]

C. DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES

1. Windows Media Digital Rights Management Technology

[186] *Id*.

[187] *See* D-VHS Certification at Appendix A ("*Format Agreement*").

[188] D-VHS Certification at 3. JVC has identified in a sample list some of the patents it holds in the United States that are essential to the design and manufacture of D-VHS products. *Id*. at Appendix A.

[189] *See* D-VHS Certification at Appendix B ("*Copy Protection Requirements*"), Appendix C ("*CPR Supplement A*").

[190] *Format Agreement* at Art. 10(2)(b).

[191] JVC Reply at 13-15, Appendices A-B.

[192] D-VHS Certification at 7.

[193] *Id*.; *Content Beneficiary Agreement* at Art. 1(D).

[194] D-VHS Certification at 11; *Content Beneficiary Agreement* at Art. 4.

[195] D-VHS Certification at 11.

[196] *Id*.

[197] *Id*.

[198] *Id*.

[199] *Id*. at 11-12.

47. Microsoft Corporation ("Microsoft") has certified its Windows Media Digital Rights Management Technology ("WMDRM") as an end-to-end digital rights management ("DRM") content protection system that can be used both for output protection as well as for secure recording and storage.[200] As an end-to-end DRM system, WMDRM is transport agnostic. Microsoft asserts that WMDRM is supported in nearly 60 consumer electronics products and more than 450 million Windows-enabled personal computers.[201] In addition, Microsoft points to the fact that major movie studios and record labels have made movie and music content available online through services using WMDRM as reflecting their support for the underlying technology.[202] Although MPAA initially disputed the applicability of content owner use or approval of WMDRM for the protection of movie content to the instant proceeding, subsequent clarifications by Microsoft on its flag-based WMDRM implementation have led MPAA and its members to express support for the approval of WMDRM under this interim process.[203]

48. WMDRM is a multi-purpose, open-platform system that can be used to protect a wide variety of audiovisual content.[204] In the case of Marked Content, WMDRM would encrypt the content and bind it to the individual device in which it was first demodulated.[205] WMDRM will also prescribe a set of usage rights that will limit the content's use and redistribution.[206] Specifically, WMDRM will allow Marked Content to be: (1) simultaneously shared among ten network streaming WMDRM-enabled devices, and (2) sent to an unlimited number of WMDRM-enabled storage devices directly connected by a USB cable, or (3) sent to a limited number of connected WMDRM-enabled storage devices over an IP-based home network.[207] Microsoft indicates that in both instances it will institute proximity controls consisting of a TTL limit of 3 and a RTT cap of 7 milliseconds or less.[208] Microsoft has committed to enabling Marked Content protected with WMDRM to be handed off to all other content protection

[200] WMDRM Certification at 1.

[201] *Id*. at 15-16.

[202] *Id*. at 13-14. Among the studios are Disney, Paramount, MGM, Sony, Universal, and Warner Brothers; the record labels include BMG, EMI, Sony, Universal, and Warner. *Id*.

[203] Opposition to the Application of Microsoft for Interim Authorization of Windows Media DRM by the Motion Picture Association of America, Inc., *et al*. at 12-13 ("MPAA Opposition to Microsoft") (stressing that a flag-based implementation of WMDRM could differ greatly from its Internet-delivered movie content implementation); Letter from C. Bradley Hunt, MPAA, and Andrew Moss, Microsoft, to Marlene Dortch, FCC at 1 (July 9, 2004).

[204] Microsoft Reply at 23.

[205] WMDRM Certification at 4. WMDRM uses a public key based management system. *Id*. at 6. Among the encryption algorithms used for portable and other media storage devices are: 56-bit RC4, 56-bit DES, 160-bit ECC El-Gamal, and 160-bit ECC-DSA. *Id*. at 7. For network devices, the algorithms include 128-bit AES and 2048-bit RSA. *Id*.

[206] *Id*. at 4-5.

[207] *Id*. at 8-10; Microsoft Reply at 5-6. The network streaming and connected devices are affirmatively authorized by the user of the originating device the first time a newly-attached network streaming or connected device requests content from the originating device. Microsoft Reply at 10-11; Letter from Mary Newcomer Williams, Covington & Burling, to Marlene Dortch, FCC at 4 (June 25, 2004) ("*Microsoft 6/25/04 Ex Parte*"); Letter from Mary Newcomer Williams, Covington & Burling, to Marlene Dortch, FCC at 2 (July 13, 2004) ("*Microsoft 7/13/04 Ex Parte*"); Letter from Mary Newcomer Williams, Covington & Burling, to Marlene Dortch, FCC at Attachment (July 15, 2004) ("*Microsoft 7/15/04 Ex Parte*"); Letter from Mary Newcomer Williams, Covington & Burling, to Marlene Dortch, FCC at 2 (July 28, 2004) ("*Microsoft 7/28/04 Ex Parte*").

[208] Microsoft Reply at 5; Letter from Gerald Waldron, Covington & Burling, and Andrew Moss, Microsoft Corporation, to Marlene Dortch, FCC at 9, 11 (May 18, 2004) ("*Microsoft 5/18/04 Ex Parte*").

systems approved by the Commission.[209]

49. WMDRM provides for revocation on a device, application, or WMDRM implementation basis.[210] In each instance, revocation occurs when the certificate of the device, application, or WMDRM implementation is compared against a list of revoked certificates at the time of authentication.[211] Revocation information is distributed with licenses for new WMDRM protected content delivered over the Internet or through physical media.[212] When a device or WMDRM implementation is revoked, the device or implementation loses access to any new WMDRM-protected content after the date of revocation but retains access to older content.[213] In the case of an application, revocation causes it to lose access to all WMDRM-protected content.[214] Revoked certificates can be renewed through a "re-individualization" process.[215] WMDRM is also extensible and upgradeable through software updates.[216]

50. WMDRM is licensed as part of the Windows Media Format Software Development Kit ("Windows Media Format SDK") and the Windows Media Rights Management Software Development Kit ("Windows Media Rights Management SDK").[217] Microsoft states that the Windows Media Format SDK and Windows Media Rights Management SDK license the use of all necessary patent claims required from Microsoft to deploy WMDRM.[218] Licensees are authorized to use WMDRM in specified applications and devices and to distribute WMDRM as an integrated component in those applications and devices.[219] Microsoft does not currently authorize third parties to implement WMDRM themselves, but plans to do so in the future.[220] Microsoft indicates that it has historically had no need to detail the specific robustness requirements applicable to WMDRM since it was directly responsible for implementation and set its own internal robustness guidelines.[221] As a result of its future plans to license third party implementations, however, Microsoft has crafted a series of detailed compliance and robustness rules applicable to personal computers, portable storage devices, and network devices.[222] Microsoft commits to

[209] Microsoft Reply at 28. Microsoft notes that the hand off of content will require the receiving technology to take a WMDRM license. *Id*. Microsoft also acknowledges that interoperability between DRM systems will require the widespread implementation of an industry standard rights expression language and expresses its commitment to the use of MPEG-21 Part 5 Rights Expression Language in this regard. *Id*.

[210] WMDRM Certification at 12; Microsoft Reply at 14. In the case of devices, Microsoft indicates that it is more common for a class of devices to be compromised. Microsoft Reply at 14. A WMDRM implementation can be in a device or in a version of Windows. *Id*.

[211] WMDRM Certification at 12; Microsoft Reply at 14-15. Microsoft provides that it may revoke DRM certificates technically or contractually on two days notice where security has been publicly or generally compromised such that Microsoft cannot reasonably remedy the breach. *See* Microsoft Certification at Appendix 13, 3(b)-(c), Ex. B ("*DRM Addendum to Windows Media Format SDK License*").

[212] Microsoft Reply at 15.

[213] *Id*.

[214] *Id*.

[215] WMDRM Certification at 17; Microsoft Reply at 11.

[216] WMDRM Certification at 10.

[217] *Id*. at 17.

[218] *Id*. at 17-18.

[219] *Id*. at 18.

[220] *Id*.; Microsoft Reply at 20-21.

[221] WMDRM Certification at 18; Microsoft Reply at 19; *Microsoft 5/18/04 Ex Parte* at 12.

[222] *Microsoft 5/18/04 Ex Parte* at 11-14; *Microsoft 6/25/04 Ex Parte* at Attachments.

complying with these same rules in its own implementations of WMDRM and in its devices and applications using WMDRM.[223]

51. Microsoft does not provide content owners or other stakeholders with a formal role in revocation decisions or change management.[224] Likewise, content owners do not receive third party beneficiary or enforcement rights with respect to the WMDRM technical specifications and compliance and robustness rules under the Windows Media Format SDK and Windows Media Rights Management SDK.[225] In lieu of these mechanisms, Microsoft pledges that it will: (1) not change its implementation of WMDRM in a manner that would afford less protection to Marked Content than set forth in its certification and related filings, (2) use its best commercially reasonable efforts to address and remedy as promptly as possible any breaches to WMDRM that diminish the protection of Marked Content, and (3) work with content owners to afford them a meaningful and reasonable role in the development and deployment of WMDRM.[226] In particular, Microsoft suggests that its Security Advisory Board can provide content owners engaged in digital media distribution with a voice in revocation and change management matters.[227]

52. Microsoft states that the Windows Media Format SDK and Windows Media Rights Management SDK are available on reasonable and nondiscriminatory terms that are broadly and publicly disclosed.[228] Microsoft also affirms that the licenses do not impose any anticompetitive obligations on WMDRM licensees.[229] Both SDKs are included at no additional cost in the Microsoft's Windows client and server licenses.[230]

2. Helix DRM Trusted Recorder

53. Helix DRM Trusted Recorder ("Helix") is another end-to-end DRM system that can be used to protect a wide range of audiovisual content across multiple platforms.[231] RealNetworks, Inc. ("RealNetworks") licenses Helix and promotes its use as a digital output protection technology in association with Marked Content.[232] RealNetworks identifies a number of consumer electronics manufacturers that have licensed its Helix DNA Client, the technology that serves as the foundation for Helix, as well as movie studios and record labels that have authorized the use of Helix for Internet distribution of video and music content.[233] Although MPAA acknowledges that content owners have

[223] *Microsoft 5/18/04 Ex Parte* at 1.

[224] Microsoft Reply at 24-26; *Microsoft 5/18/04 Ex Parte* at 14-15.

[225] Microsoft Reply at 26-27; *Microsoft 5/18/04 Ex Parte* at 14-15.

[226] *Microsoft 5/18/04 Ex Parte* at 14-15.

[227] Microsoft Reply at 24-25.

[228] WMDRM Certification at 17.

[229] Microsoft Reply at 29.

[230] WMDRM Certification at 17.

[231] Letter from Laura Philips, Drinker Biddle & Reath, LLP, to Marlene Dortch, FCC, at 2 (June 18, 2004) ("*RealNetworks 6/18/04 Ex Parte*").

[232] RealNetworks Reply at 3.

[233] Licensees of Helix DNA Client include Hitachi, IBM, Intel, Motorola, NEC, Sharp, Sony, Sun Microsystems, Texas Instruments, and Toshiba. Helix Certification at 45. Among the studios authorizing the Internet distribution of movie content through Helix-based MovieLink are MGM, Paramount, Warner Brothers, Universal and Sony. *Id*. at 41-42; RealNetworks Reply at 11-12. Similarly, RealNetworks identifies Universal Music, Sony Music, EMI, BMG, and Warner Brothers Music as having approved Helix DRM in association with the Internet distribution of their music. *Id*.

authorized the delivery of movie content through commercial services that utilize Helix, such as Movielink, it emphasizes that Helix would be implemented in a different manner for digital broadcast television content and that content owners have yet to use or approve Helix in this context.[234]

54. When Marked Content is received and demodulated by a Helix-compliant device, it will encrypt the content and bind it to the device in association with the Helix Device DRM software, which is referred to as a "Trusted Recorder."[235] The Trusted Recorder will only allow protected content to be accessed in a usable form by itself or a Helix-compliant device that it has validated, also referred to as a "Trusted Client."[236] A validation process is used to associate a Trusted Recorder with up to 10 Trusted Clients for a six month time frame, and that validation is authenticated by the Trusted Recorder prior to playback.[237] Each Trusted Client may only hold the validation from a single Trusted Recorder at a time, and it must be renewed at the end of each six month period to avoid automatic deletion.[238] In addition, RealNetworks indicates that it will further restrict the scope of redistribution through the imposition of TTL and RTT proximity controls and by limiting the output of protected content to Commission-approved protection technologies.[239]

55. Helix has the ability to revoke at both the content and component level.[240] Content revocation invalidates the key used by a particular Trusted Recorder to encrypt content, thereby rendering all content associated with that Trusted Recorder unusable.[241] Component revocation affects a Helix application, such as a Trusted Recorder or a Trusted Client.[242] When the playback of content and authentication is initiated, the digital signature of each component that will handle decrypted data is verified against a secure database of revoked signatures residing in the Trusted Recorder or Trusted Client.[243] If the digital signature of a component appears in the database, validation and playback will fail.[244] Revocation information can be disseminated in content delivered through the Internet or in physical media.[245] Revoked devices or applications can be renewed through software upgrades delivered by similar means.[246]

56. RealNetworks licenses Helix as a part of its Helix Device DRM Software Development

---

[234] Opposition to the Application of RealNetworks Inc. for Interim Authorization of Helix DRM Trusted Recorder and Helix Device DRM by the Motion Picture Association of America, Inc., *et al*. at 10-11 ("MPAA Opposition to RealNetworks")

[235] RealNetworks Reply at 3. A 128-bit AES algorithm or its equivalent is used in the encryption process. *Id*.

[236] RealNetworks Reply at 4; *RealNetworks 6/18/04 Ex Parte* at 4-6.

[237] Helix Certification at 27-33; RealNetworks Reply at 4; *RealNetworks 6/18/04 Ex Parte* at 4. Letter from Laura Philips, Drinker, Biddle & Reath, LLP, to Marlene Dortch, FCC at 3-4 (July 1, 2004) ("*Real Networks 7/1/04 Ex Parte*").

[238] RealNetworks Reply at 3-4.

[239] *Id*. at 4; *RealNetworks 6/18/04 Ex Parte* at 3, 8. RealNetworks will impose a TTL limit of 3 and a RTT limit of 7 milliseconds or less. *RealNetworks 7/1/04 Ex Parte* at 2.

[240] RealNetworks Reply at 8; *RealNetworks 6/18/04 Ex Parte* at 5.

[241] RealNetworks Reply at 8; *RealNetworks 6/18/04 Ex Parte* at 5.

[242] RealNetworks Reply at 8; *RealNetworks 6/18/04 Ex Parte* at 5.

[243] RealNetworks Reply at 8-9; *RealNetworks 6/18/04 Ex Parte* at 4, 6.

[244] RealNetworks Reply at 9; *RealNetworks 6/18/04 Ex Parte* at 6.

[245] RealNetworks Reply at 9; *RealNetworks 6/18/04 Ex Parte* at 6.

[246] RealNetworks Reply at 10; *RealNetworks 6/18/04 Ex Parte* at 6.

Kit ("Helix Device DRM SDK").[247] Licensees are granted the right to use and distribute Helix as part of a bundle of associated software applications and are required to comply with both the Commission's flag compliance and robustness rules, as well as those imposed by RealNetworks.[248] The Helix Device DRM SDK license does not provide for content owner participation in change management or grant third party beneficiary enforcement rights.[249] RealNetworks reserves the right to change the functionality or pricing of the Helix Device DRM SDK at any time, but commits to making any such changes on a reasonable and non-discriminatory basis.[250] RealNetworks further asserts it will license Helix for the specific purpose of protecting Marked Content on a reasonable and non-discriminatory basis for all similarly situated companies and that its license fees will be structured as a per unit royalty arrangement to encourage the availability of low cost devices.[251]

3. SmartRight

57. Like WMDRM and Helix, the SmartRight technology ("SmartRight") recently developed by Thomson Inc. and its partners (collectively, "Thomson") is an end-to-end DRM system that can be used to protect marked digital broadcast television and other audiovisual content.[252] SmartRight differs from its DRM counterparts in that it protects content within a smart card-based domain of authorized devices known as a Personal Private Network ("PPN").[253] Licensing of SmartRight will be administered by the SmartRight Licensing Authority, LLC.[254] Thomson promotes SmartRight as a technology that will permit consumers to copy freely, use and enjoy digital broadcast content within the PPN.[255] On the basis of certain commitments made by Thomson, MPAA supports SmartRight's certification under this interim process.[256]

58. Under the SmartRight model, protected content can be shared among devices in a PPN consisting of up to ten display devices and an unlimited number of reception or secure storage devices.[257] Although SmartRight can be configured to authorize remote devices to a PPN through an IP network or over the Internet, Thomson initially commits to requiring physical propagation of the PPN through the direct insertion of an authorized smart card into new display devices.[258] When a SmartRight reception device demodulates Marked Content, it encrypts the content and encodes it as a "private copy" which

[247] RealNetworks Reply at Attachment ("*Helix Device DRM SDK License*")

[248] *Helix Device DRM SDK License* at §§ 2-3, Appendix D.2-D.3; RealNetworks Reply at 11.

[249] RealNetworks Reply at 10-11.

[250] *Helix Device DRM SDK License* at § 6(c) (providing that RealNetworks cannot unilaterally change licensees' royalty or financial obligations); *RealNetworks 6/18/04 Ex Parte* at 7.

[251] Helix Certification at 45; RealNetworks Reply at 12; *RealNetworks 6/18/04 Ex Parte* at 7.

[252] SmartRight Certification at 2. Thomson developed SmartRight in coordination with its partners Axalto, Gemplus SA, Micronas, Nagravision SA, Pioneer Corporation, SCM Microsystems, and ST Microelectronics N.V. *Id*. at 26.

[253] *Id*. at 1, 12.

[254] *Id*. at Appendix A.

[255] *Id*. at 3. Thomson also points out that through use of a SmartRight set top box, consumers can preserve the functionality of their legacy analog equipment. *Id*. at 11, 21.

[256] Letter from C. Bradley Hunt, MPAA, and David Arland, Thomson, to Kenneth Ferree, FCC at 3 (May 28, 2004) ("*Thomson 5/28/04 Ex Parte*").

[257] Thomson Reply at 9, n.17.

[258] *Id*.

may only be viewed within the PPN linked to the reception device.[259] Protected content cannot be accessed in a usable format on any device outside that specific PPN, including devices linked to other SmartRight PPNs.[260] Thomson indicates that SmartRight can permit consumers to access content at a remote location linked to their PPN, such as a second home, office, or boat.[261] In response to concerns articulated by MPAA, however, Thomson has committed to implement TTL and RTT proximity controls on an interim basis.[262] Thomson also specifies that SmartRight is interface neutral and will receive digital broadcast television content from, and export to, other Commission-approved protection technologies.[263]

59. SmartRight permits revocation at three levels – PPN, smart card, and display device.[264] Lists identifying revoked keys and authorizations are created by the SmartRight Association, a not-for-profit corporation representing the interests of content providers and adopters, and are distributed in content.[265] Although the SmartRight Association is responsible for revocation decisions, content participants may request revocation.[266] SmartRight can also effectuate renewal of its entire security schema through smart card replacement, a measure which content participants can request.[267]

60. The licensing regime for SmartRight consists of two components, an adopter agreement and a content participant agreement.[268] Adopters who possess essential patent claims have the option to either agree to not assert those claims against fellow adopters or to license them on a reasonable and non-discriminatory basis.[269] Thomson describes the applicable compliance and robustness requirements as generally following the Commission's flag rules.[270] SmartRight's change management terms do not

[259] SmartRight Certification at 9. SmartRight uses 112-bit Triple DES for content scrambling, 128-bit AES for individual device communications and identification, 1024 or 2048-bit RSA for authentication and SHA1 hash function for verification. *Id*. at 16.

[260] *Id*. at 8.

[261] *Id*.

[262] *Thomson 5/28/04 Ex Parte* at 2; Letter from David Arland, Thomson, to Marlene Dortch, FCC at 2 (June 23, 2004) ("*Thomson 6/23/04 Ex Parte*"). The specific proximity controls consist of a TTL limit of 3 and a RTT limit of 7 milliseconds or less. *Thomson 5/28/04 Ex Parte* at 2.

[263] SmartRight Certification at 20.

[264] *Id*. at 2-3, 11, 18-19. Revocation may be applied in four instances: (1) where a device key has been copied such that it is found in more than one device or product; (2) where a key has been lost, stolen, intercepted or otherwise misdirected, or is made public or disclosed; (3) where a network key is present in more terminal modules than permitted by the maximum network size; or (4) it is required by court order, or other competent government authority. *See* Thomson Reply at Appendix A, Art. IV ("*SmartRight Adopter Agreement*"); *see also* Thomson Reply at Appendix B, § 5.3.2 ("*SmartRight Content Participant Agreement*").

[265] SmartRight Certification at 11, 24.

[266] Thomson Reply at 12. Content participants must provide the SmartRight Association with proof that one of the four revocation criteria has been met. *SmartRight Content Participant Agreement* at § 3.2, 5.3.1. Where proven, revocation must be initiated. *Id*.

[267] SmartRight Certification at 10, 18; Thomson Reply at 13. The SmartRight Association can institute renewal where: (1) unauthorized use or distribution of SmartRight content have reached a sufficient level to justify the cost of renewal; (2) it is feasible to upgrade the reliability and security of SmartRight; and (3) a requirement exists to implement a change in outstanding smart cards by court order, or other competent government authority. SmartRight Certification at 18; *see also SmartRight Adopter Agreement* at § 3.2, 4.3; *SmartRight Content Participant Agreement* at §§ 5.3.1, 5.3.4.

[268] Thomson Reply at 4.

[269] SmartRight Certification at 23; *SmartRight Adopter Agreement* at § 5.5.

[270] SmartRight Certification at 22, 25; *SmartRight Adopter Agreement* at Ex. B, C.

permit material changes to the technical specification or compliance rules that would materially increase the cost or complexity of compliance products, unless mandated by the Commission or other governmental authority.[271] Other changes are permitted upon notice to adopters, providing them with an opportunity to resolve objections, and allowing for a reasonable implementation period.[272] Content participants can object to any changes that would have a material and adverse effect on the integrity or security of the SmartRight system, as well as other changes to the adopter agreement and its compliance rules.[273] Third party beneficiary rights are also available to content participants to enforce the terms of the adopter agreement.[274] Thomson asserts that SmartRight will be licensed on a reasonable and non-discriminatory basis.[275] Adopters are responsible for an annual license fee, per unit royalties, and certified key fees.[276] Content participants must pay an annual administration fee.[277] Changes to the fees must be commensurate with administrative costs.[278]

III. DISCUSSION

61. Although each certification raises issues that are germane to its subject technology, certain commonalities also exist among the various filings which merit a uniform resolution. In particular, the oppositions and responses filed by MPAA with respect to each certification echo similar themes and topics.[279] We consider these common issues below in a consolidated fashion in an effort to streamline our evaluation of each content protection technology and recording method. We again reiterate that our goal in this proceeding is to establish a redistribution control system that will prevent the

[271] SmartRight Certification at 24; *SmartRight Adopter Agreement* at § 3.3.2.

[272] SmartRight Certification at 24; *SmartRight Adopter Agreement* at Art. 3.

[273] Thomson Reply at 14; *SmartRight Content Participant Agreement* at § 3.6.

[274] Thomson Reply at 11; *SmartRight Adopter Agreement* at § 10.4, Ex. A at § 3; *SmartRight Content Participant Agreement* at § 3.3.

[275] SmartRight Certification at 22.

[276] Adopters must pay a $10,000 annual fee for an evaluation license, with a $30,000 fee to convert to a full production license. *Id*. at 23; *SmartRight Adopter Agreement* at § 2.2-2.5, Ex. A. The per unit royalty is $2, and the certified key fee is $0.10. *Id*.

[277] The administration fee is $30,000. *SmartRight Content Participant Agreement* at § 4.1, Ex. A.

[278] *SmartRight Adopter Agreement* at § 2.1; *SmartRight Content Participant Agreement* at § 4.1.

[279] *See* Comments Pertinent to all Filings for Interim Certification Submitted by the Motion Picture Association of America, Inc., *et al*. ("MPAA Common Comments"); Response to the Application of Sony Corporation for Interim Authorization of MagicGate by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to Sony"); Opposition to the Application of Thomson, *et al.* for Interim Authorization of SmartRight by the Motion Picture Association of America, Inc., *et al*. ("MPAA Opposition to Thomson"); Response to the Application of Philips Electronics North America Corp. and Hewlett-Packard Co. for Interim Authorization of Vidi Recordable DVD Protection System by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to Philips and HP"); Response to the Application of Digital Content Protection, LLC for Interim Authorization of High Bandwidth Digital Content Protection by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to DCP"); Response to the Application of 4C Entity LLC for Interim Authorization of Content Protection Recordable Media for Video Content by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to 4C"); MPAA Opposition to TiVo; Response to the Application of Digital Transmission Licensing Administrator LLC for Interim Authorization of Digital Transmission Content Protection by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to DTLA"); MPAA Opposition to RealNetworks; MPAA Opposition to Microsoft; Response to the Application of Victor Company of Japan for Interim Authorization of D-VHS by the Motion Picture Association of America, Inc., *et al*. ("MPAA Response to JVC"). MPAA filed a motion asking that its late-filed oppositions and responses be accepted as timely. *See* Motion to Accept Late-Filed Comments as Timely (filed April 12, 2004). We hereby grant MPAA's motion.

mass indiscriminate redistribution of digital broadcast television content.

A. SCOPE OF APPROVAL

62. The Commission established this interim process to expeditiously approve content protection and recording methods so that manufacturers could produce flag-compliant devices in the near term while additional comment was sought on the appropriate structure of a permanent approval process.[280] MPAA has interpreted the use of the word "interim" in this context to mean that Commission determinations made under this process would themselves be interim in nature and subject to potential reevaluation once a permanent approval mechanism is established.[281] This interpretation is inconsistent with our intent in the *Broadcast Flag Order* – our use of the word "interim" therein referred to the nature of the process itself and not the scope of any resulting approval or disapproval determinations. Indeed, we believe that there would be significant marketplace uncertainty if we were to do otherwise. If our approvals under this interim process were provisional in nature, and an approved technology were later disapproved under the final approval process, manufacturers and consumers could be stranded with potentially incompatible legacy products. We therefore clarify that once a particular content protection technology or recording method has been approved for broadcast flag purposes under this interim process, such approval remains valid unless (1) the underlying technology or its license terms have been altered in a manner that triggers our change management oversight, or (2) the approval is revoked pursuant to Section 73.9008(e) of the Commission's rules.[282]

63. At this juncture, we also wish to clarify the substantive scope of our review under this interim process. We recognize that nearly all of the content protection technologies and recording methods that are the subject of the above-referenced certifications were created prior to adoption of the *Broadcast Flag Order*. As such, most are capable of expressing varying degrees of protection for different types of content. For example, DTCP can encode digital content with CCI ranging from no authentication or encryption of unmarked broadcast content up to "Copy Never" for prerecorded media or premium pay television content.[283] Some technologies, such as CPRM, impose content protection requirements on analog outputs and anticipate the future adoption of watermarking technology to protect digital audio and video content.[284] Other protection systems, such as WMDRM, are used by various industry segments and governments to protect both commercial and non-commercial content.[285]

64. We are mindful that the digital broadcast content protection lens through which we are viewing these technologies focuses on a small subset of their capabilities. In light of this fact, our analysis and review of the above-referenced certifications must maintain a similar perspective. We are reviewing these technologies solely for their suitability in protecting digital broadcast television content as a part of the redistribution control system we established in the *Broadcast Flag Order*. To the extent that certain of these technologies may be intended for use in unidirectional digital cable ready products to protect pay television programming, initial approval determinations are made by CableLabs under the interim policy adopted in our recent *Second Report and Order and Second Further Notice of Proposed*

[280] *Broadcast Flag Order*, 18 FCC Rcd at 23575, 23578-79.

[281] *See, e.g.*, MPAA Common Comments at 2.

[282] 47 C.F.R. § 73.9008(e). *But see infra* ¶ 91 (providing that the Commission may reconsider its decision on the technologies' applicable license terms as the result of judicial or regulatory determinations as the market develops).

[283] DTCP Certification at 6-7.

[284] CPRM Certification at 7, Ex. 1 at 83.

[285] Microsoft Reply at 23.

Rulemaking relating to digital cable compatibility.[286] Our approval of these thirteen technologies for broadcast flag purposes should, therefore, not be interpreted as constituting a review or decision on the merits with respect to their applicability to analog content protection, the protection of non-broadcast digital television content, or their suitability for use in other contexts. To the extent that MPAA and Philips advocate Commission action on matters relating to these extrinsic subjects, we decline to take action.[287] We remain nonetheless deeply concerned about the potential extension of our redistribution control content protection system for digital broadcast television into areas outside the intended scope of the *Broadcast Flag Order*. We will closely monitor the deployment of these content protection technologies and recording methods as they relate to digital broadcast television content and will take action as needed to ensure that such aggrandizement does not occur.

65. Another area in which technology proponents and commenters have sought clarification relates to whether an approval by the Commission of a particular content protection technology or recording method covers some or all of the transports or media used by that technology, whether they are currently in use or may be adopted in the future. As described above, DTCP has been mapped to a number of diverse transports including physical connectors such as IEEE 1394 and USB, and IP wired and wireless technologies including 802.11 and Ethernet.[288] CPRM has similarly been designed for different types of removable consumer recording media, including DVD-R/-RW, SD Memory Cards, and Secure CompactFlash.[289] DRM technologies, however, are typically transport agnostic, rendering this issue inapplicable to WMDRM, Helix and SmartRight.

66. Philips argues that DTCP, CPRM, and HDCP should only be approved on an interface-by-interface or media-by-media basis where the applicable technology is specifically defined for that interface or media.[290] Philips states that it is not uncommon for the mapping of a content protection technology or recording method to a new transport or media to necessitate legal and technical modifications.[291] If such changes were permissible without Commission review or oversight, Philips suggests that technology proponents could, once having received the Commission's approval for one particular technology, declare an entirely new and different content protection technology or recording

[286] *See Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment*, 18 FCC Rcd 20885, 20919-20 (2003). Initial determinations made by CableLabs are subject to Commission review in cases of dispute. *Id*. The *Second Further Notice of Proposed Rulemaking* seeks comment on the appropriate standards and procedures to be used in a permanent approval process for content protection technologies used in unidirectional digital cable ready products. *Id*. at 20921-22. We expect that technologies submitted to CableLabs will receive a timely and fair review process similar to that conducted here. The lack of a timely, fair and neutral process for the approval of non-broadcast content will set back parties who seek to manufacture devices for both broadcast and non-broadcast content.

[287] *See e.g.*, MPAA Response to 4C at 4-5 (seeking various technical revisions to the CPRM adopter agreement relating to audio content, as well as the reinstitution of an obligation for devices to detect and respond to CGMS-A and Macrovision on the recording of analog video signals); Philips Opposition to 4C at 31-32, 34-35 (arguing in favor of: (1) an extension of the right to use VGA outputs for "copy no more" content from computer products to consumer electronics products, and (2) the elimination of certain provisions relating to the CPRM compliance rules applicable to audio content); and Philips Opposition to DTLA at 33-34 (arguing in favor of an extension of the right to use VGA outputs for "copy no more" content from computer products to consumer electronics products).

[288] DTCP Certification at 3.

[289] CPRM Certification at 3.

[290] Philips Opposition to DTLA at 36-37; Philips Opposition to 4C at 33; Philips Opposition to DCP at 20-21.

[291] Philips Opposition to DTLA at 36-37; Philips Opposition to 4C at 33; Philips Opposition to DCP at 20-21.

method to fall within the confines of the earlier approval.[292]

67. DTLA, 4C and DCP each dispute Philips' claims.[293] DTLA asserts that DTCP's encryption and authentication works the same over every interface protocol with an equal level of robustness.[294] As a practical matter, DTLA indicates that it would be technically infeasible to differentiate Marked Content from similarly encoded content once it enters the DTCP encryption system and it would therefore be impossible to control the ability of that Marked Content to only pass through certain approved interfaces.[295] DTLA interprets PHILA as providing a blanket approval to DTCP for all current and future transports to which it may be mapped.[296] 4C states that CPRM's extensibility to multiple recordable media formats is one of its most important features and consumers should not be denied the right to use these new formats.[297] Where CPRM's essential attributes remain as they are in the certification before the Commission, 4C believes there is no reason to expect that content will not be protected at the same level and therefore no need exists for the Commission to conduct a reiterative proceeding.[298] DCP maintains that a metered approach to approvals would not be a good policy position for the Commission to take and suggests that Philips' support for this approach reflects its own interest in the licensing of HDMI as a transport for use with HDCP.[299]

68. Although we agree with 4C that where a content protection technology or recording method's essential attributes remain unchanged by its mapping to a new transport content is likely to be protected at the same level, we ultimately conclude that our review and approval of these technologies must be based on a transport-by-transport or media-by-media basis. As demonstrated by the mapping of DTCP to IP, significant legal and technical changes can result from this process.[300] We are therefore reluctant to issue a blanket approval for all existing and future transports or media to which these thirteen technologies may be mapped. At the same time, we do not wish to inhibit innovation or prevent consumers from benefiting from technological advances. We will therefore consider a proposal by a technology proponent for the addition of new a transport or media as a material change and an amendment to their existing certification. We will process any such amendments on an expedited basis following public notice and comment.[301] When evaluating these amendments, we will not reconsider any issues in the underlying certification that have already been addressed in this *Order,* unless they are directly impacted or modified by the mapping to the new transport or media. We believe that this approach will streamline the amendment process where any changes are *pro forma* in nature, but will allow for a full review of the merits where more substantive modifications occur. In the case of DTCP, we are not persuaded that this transport-by-transport approach will present any significant technical

[292] Philips Opposition to DTLA at 36-37; Philips Opposition to 4C at 33; Philips Opposition to DCP at 20-21.

[293] DTLA Reply at 56; 4C Reply at 19; DCP Reply at 17-18.

[294] DTLA Reply at 56.

[295] *Id*.

[296] *Id*.

[297] 4C Reply at 19.

[298] *Id*.

[299] DCP Reply at 17-18.

[300] *See* Philips Opposition to DTLA at 29-30; DTLA Reply at 50-54 (discussing the various legal and technical changes resulting from the mapping of DTCP to Internet Protocol, including a decrease in the number of authorized sink devices from 62 to 34, a switch in cipher from M6 to AES, and the addition of discussions on localization requirements).

[301] Technology proponents may certify any amendments pursuant to our procedures for subsequent certifications. *See* 47 C.F.R. § 73.9008(c).

difficulties given that it has been emulated in the DFAST and the Content Scramble System ("CSS") licenses and certain implementations of DTCP, such as over IP, have not yet been deployed in the marketplace.[302]

B. SCOPE OF REDISTRIBUTION CONTROL

1. Localization

69. In adopting a redistribution control system for digital broadcast television, the Commission articulated the express goal of the *Broadcast Flag Order* as:

> [P]revent[ing] the indiscriminate redistribution of [digital broadcast television] content over the Internet or through similar means. This goal will not (1) interfere with or preclude consumers from copying broadcast programming and using or redistributing it within the home or similar personal environment as consistent with copyright law, or (2) foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution.[303]

The Commission then sought further comment on the appropriate scope of redistribution that should be prevented and whether it was useful to define a personal digital network environment ("PDNE") within which consumers could freely redistribute digital broadcast television content.[304]

70. Although MPAA and other parties have filed comments responding to the *Further Notice of Proposed Rulemaking* on the appropriate scope of redistribution,[305] MPAA has also raised this issue in oppositions and responses it has filed with respect to certain certifications where the redistribution of content is not otherwise constrained through the inherent limitations of physical connectors or media.[306] Specifically, MPAA advocates the adoption of "localization" constraints by DTLA, Microsoft, RealNetworks, Thomson, and TiVo that would effectively restrict the scope of content redistribution to a tightly defined physical space in and around the home.[307] MPAA clarifies that it is not opposed to the concept of remote access in principle, but that a number of technological, policy, privacy and legal questions must be addressed before it can be implemented.[308]

71. The technology proponents have answered MPAA's request for localization constraints in different ways. DTLA currently requires adopters implementing DTCP over IP to limit TTL to a value

[302] Letter from Jonathan Rubin, American Antitrust Institute, to Marlene Dortch, Secretary, FCC at Attachment A (May 28, 2004) ("*AAI Ex Parte*").

[303] *Broadcast Flag Order*, 18 FCC Rcd at 23555.

[304] *Id*. at 23578.

[305] *See e.g.*, MPAA Comments, MB Docket 02-230 (filed Feb. 13, 2004); MPAA Reply Comments, MB Docket 02-230 (filed Mar. 15, 2004).

[306] *See* MPAA Opposition to Thomson at 3-6; MPAA Opposition to TiVo at 4-6; MPAA Opposition to RealNetworks at 3-7; MPAA Opposition to Microsoft at 3-6; and MPAA Response to DTLA at 3.

[307] *See* MPAA Opposition to Thomson at 3-6; MPAA Opposition to TiVo at 4-6; MPAA Opposition to RealNetworks at 3-7; MPAA Opposition to Microsoft at 3-6. In the case of DTCP, MPAA recognizes that DTLA has established a localization work plan to identify proximity requirements for DTCP over IP and asks that this work plan be included in DTCP's certification. MPAA Response to DTLA at 3.

[308] *See* MPAA Opposition to Thomson at 3-6; MPAA Opposition to TiVo at 4-6; MPAA Opposition to RealNetworks at 3-7; MPAA Opposition to Microsoft at 3-6; MPAA Response to DTLA at 3; Letter from Bruce Boyden, Proskauer Rose LLP, to Marlene Dortch, FCC at Attachment (July 16, 2004).

of 3.[309] Pursuant to its recently completed localization work plan for DTCP over IP, DTLA has also committed to institute a RTT limit of 7 milliseconds or less in order to constrain the redistribution of content within an area approximating the home.[310] Microsoft specifies that it will adopt these same TTL and RTT limits in an effort to keep Marked Content proximate to the original device where it is encrypted by WMDRM.[311] RealNetworks has made a similar commitment with respect to Helix.[312] Thomson provides a more qualified response – Thomson will tentatively adopt a RTT limit of 7 milliseconds and a TTL limit of 3 for its SmartRight technology, but allows that these controls can later be relaxed should content owners agree or the Commission's rules so permit.[313] Unlike DTLA, Microsoft, RealNetworks, and Thomson, TiVo declines to adopt any proximity controls for its TiVoGuard technology and argues that such controls fall outside the scope of this proceeding.[314]

72. Although we will address the scope of redistribution issue in a broader context as part of our resolution of the *Further Notice of Proposed Rulemaking*, we are not inclined as part of our review of these certifications to impose proximity controls as an additional obligation where other reasonable constraints sufficiently limit the redistribution of content. The Commission's stated goal in the *Broadcast Flag Order* is clear – to prevent the indiscriminate redistribution of digital broadcast television content over the Internet or through similar means. Our goal was not to prevent "unauthorized" redistribution as advanced by MPAA.[315] Rather, we explicitly provided that the scope of the *Broadcast Flag Order* "does not reach existing copyright law."[316] We conclude that SmartRight and TiVoGuard each meet the Commission's stated goal of preventing indiscriminate redistribution through different combinations of device limits, interactive device authentication, and affinity-based mechanisms. With respect to TiVoGuard, we note in particular that under the terms of TiVo's subscriber agreement, copyrighted content may only be used for personal, non-commercial purposes.[317] The limit of 10 devices uniquely associated with a single secure viewing group additionally prevents content from being indiscriminately redistributed in a "daisy chain" fashion.[318] In the case of SmartRight, the smart card-based PPN structure and associated cap of 10 display devices performs a similar limiting function.[319] It is our hope that both TiVoGuard and SmartRight will not only provide a reasonable level of redistribution control for digital broadcast content, but will also facilitate new and innovative consumer uses, such as remote access to content. We recognize that MPAA and the National Football League ("NFL") have expressed concerns regarding the impact of remote access on local and regional broadcast television markets.[320] Given the

[309] *See* DTCP Volume 1, Supplement E, Mapping DTCP to IP (Information Version) at 18, *filed in* Letter from Seth Greenstein, McDermott, Will & Emery, to Marlene Dortch, FCC (May 5, 2004).

[310] DTLA Reply at 3; *DTLA 6/1/04 Ex Parte* at Attachment; *DTLA 7/20/04 Ex Parte* at 2; *DTLA 7/22/04 Ex Parte* at 1-2.

[311] Microsoft Reply at 5; *Microsoft 5/18/04 Ex Parte* at 9, 11.

[312] *RealNetworks 7/1/04 Ex Parte* at 2.

[313] Thomson Reply at 7-8; *Thomson 6/23/04 Ex Parte* at 2.

[314] TiVo Reply at 21-24.

[315] *See e.g.*, MPAA Opposition to TiVo at 3 (asserting that "TiVoGuard fails to sufficiently protect against unauthorized redistribution of Marked and Unscreened Content because it does not include any distance-based limitations on transmissions of the content").

[316] *Broadcast Flag Order,* 18 FCC Rcd at 23555.

[317] *TiVo 7/28/04 Ex Parte* at Attachment.

[318] TiVoGuard Certification at 25; *TiVo 7/21/04 Ex Parte* at Attachment.

[319] Thomson Reply at 9, n.17.

technical limits and affinity-based parameters of SmartRight and TiVo's TiVoToGo implementation, we believe that these concerns are speculative and irrelevant to our stated goal of preventing indiscriminate redistribution.[321]

73. In contrast, WMDRM and Helix lack the affinity-based linkage and interactive device authentication present in SmartRight and TiVoGuard.[322] We recognize, however, that both Microsoft and RealNetworks have committed to implement a combination of TTL and RTT limits to restrict the scope of redistribution. We conclude that this combination, as implemented by Microsoft and RealNetworks in conjunction with their WMDRM and Helix technologies, represents an adequate limiting mechanism. We emphasize that this determination is predicated on the specific parameters outlined by Microsoft and RealNetworks in their certifications and subsequent filings in these proceedings. We believe that determinations of whether proximity controls are necessary or desirable must be made on a case-by-case basis, taking into account the nature of the underlying content protection technology, whether it utilizes any other limits on the scope of redistribution, and the manner in which it would implement proximity controls.

74. In the case of DTCP over IP, we conclude that the combination of existing TTL and proposed RTT limits will adequately restrict the scope of redistribution.[323] Our approval of DTCP over IP is conditioned, however, on DTLA submitting to the Commission final revisions to its mapping specification for DTCP over IP reflecting its proposed RTT requirements.[324] Although adopters will not be required to implement these revisions until 18 months after the DTCP over IP specification becomes final, we clarify that only implementations of DTCP over IP using a combination of TTL and RTT limits are authorized for use with Marked Content.[325] We also specify that our approval of localization constraints for DTCP is limited to its IP implementation and does not extend to other transports to which DTCP has been mapped. Should DTLA determine that, pursuant to its ongoing localization work plan for other protocols, proximity controls are desired for non-IP transports, it must submit any such proposal to

(...continued from previous page)

[320] *See e.g.*, MPAA Opposition to TiVo at 5-6; Letter from Frank Hawkins, NFL, to Rick Chessen, FCC at 1-2 (June 24, 2004) (speculating that without "any constraints on the timing of redistribution … [TiVoToGo and Helix] users presumably would be able to redistribute games *as* they are broadcast," thereby upsetting the NFL's regional television plan).

[321] *See* Letter from James Burger, Dow, Lohnes & Albertson, to Rick Chessen, FCC at 1-3 (June 30, 2004) (indicating that "TiVo remote access does not permit real-time retransmission of a three-hour football game or anything remotely analogous").

[322] Microsoft and RealNetworks also utilize device limits as part of their systems. Microsoft's network streaming device implementation of WMDRM imposes a 10 device limit, while its connected storage device implementation restricts the transfer of content over IP to a "limited number" of devices. Microsoft Reply at 5-6; *Microsoft 5/18/04 Ex Parte* at 9, 11; *Microsoft 7/13/04 Ex Parte* at 2; *Microsoft 7/15/04 Ex Parte* at Attachment. No such limit is used in Microsoft's connected storage device implementation where the devices are directly connected via USB. *Id*. RealNetworks limits the number of Trusted Clients associated with a specific Trusted Recorder during any six month period to 10. *RealNetworks 7/1/04 Ex Parte* at 3.

[323] DTLA also imposes a 34 sink device limit for DTCP over IP. DTCP Certification at 10.

[324] *See DTLA 7/20/04 Ex Parte* at 2; *DTLA 7/22/04 Ex Parte* at 1.

[325] *See DTCP Adopter Agreement* at § 3.3. We do not believe that TTL alone is an adequate tool to restrict the scope of redistribution given its susceptibility to circumvention. Absent some associated form of proximity control, TTL can be circumvented through the use of a Virtual Private Network to encapsulate IP packets so that the TTL field is not decremented in transmission. *See* Letter from James Burger, Dow, Lohnes & Alberston, PLLC, to Susan Mort, FCC at Attachment at 6-7 (June 22, 2004), *accord* Letter from Bruce Boyden, Proskauer Rose, LLP, to Marlene Dortch, FCC at Attachment at 9 (July 16, 2004) ("TiVo merely states the obvious when it argues that TTL alone is not difficult to circumvent").

the Commission for evaluation as a material change to its certification.[326]

2. Copy Restrictions

75. As reflected above, our interest in maintaining the proper balance between protecting digital broadcast content and promoting its use and enjoyment by consumers remains paramount. We continue to believe that, as stated in the *Broadcast Flag Order*, a redistribution control content protection system for digital broadcast television will not interfere with or preclude consumers from copying, using or redistributing digital broadcast television content as consistent with copyright law.[327] We recognize, however, that certain of the above-referenced content protection technologies and recording methods are unable to effectuate redistribution control through means other than copy restraints. For example, the D-VHS format encodes all content at the time of recording as "copy restricted" in CGMS, which would effectively limit broadcast content to one generation of copies.[328] Likewise, since HDCP is used to protect uncompressed video that generally cannot be copied by today's consumer equipment due to data stream size, HDCP was not designed to express different content protection states, such as redistribution control, and its adopter agreement was crafted with an explicit prohibition on copying.[329]

76. We must again acknowledge that the majority of these thirteen content protection technologies and recording methods were developed prior to adoption of the *Broadcast Flag Order*. As such, they carry with them certain legacy attributes that, while less than ideal from a broadcast flag perspective, may have been appropriate or necessary at the time and in the context that they were developed. The specific uses for which D-VHS and HDCP were developed – namely, the recording of HD digital content and the transport of uncompressed digital video content to a display – represent in their own right important pro-consumer elements of the digital transition. We are thus disinclined to prohibit D-VHS and HDCP for broadcast flag purposes, particularly where other output protection technologies and recording methods exist that permit copying and promote the use and enjoyment of digital broadcast television content by consumers. We are encouraged that a recent modification to the D-VHS copy protection requirements permits manufacturers to create D-VHS products that output protected digital broadcast content with "copy one generation" DTCP encoding, allowing a consumer to link two D-VHS devices and make additional protected copies.[330] We approve the D-VHS certification on the condition that JVC requires its adopters to implement this modification to ensure that consumers enjoy the maximum flexibility of its D-VHS technology.

77. We wish to clarify, however, that our approval of D-VHS and HDCP should not be interpreted as precedent supporting the future adoption of technologies that impose copy restrictions on digital broadcast television content. By the same token, it is not our intent to hinder competitors to D-VHS and HDCP from entering this market. We will therefore not consider the existence of copy restrictions to *per se* prevent an output protection technology or recording method's approval for broadcast flag purposes, particularly where the technology was developed prior to the adoption of the *Broadcast Flag Order*. Rather, we will consider such restrictions as a factor weighing strongly against the technology's approval as a part of our consideration of the functional criteria contained in Section

[326] *See DTLA 7/20/04 Ex Parte* at 1-2; 47 C.F.R. § 73.9008(c).

[327] *Broadcast Flag Order*, 18 FCC Rcd at 23555.

[328] D-VHS Certification at 11. JVC indicates that a format cognizant D-VHS device could permit the making of subsequent generations or copies for flag-marked or EPN encoded content. *Id*.; *see also* JVC Reply at 6-9.

[329] HDCP Certification at 5; *DCP 6/25/04 Ex Parte* at 1-3.

[330] The D-VHS copy protection requirements now enable format non-cognizant devices to read embedded CCI and the EPN indicator and convert it to "copy one generation" when outputting to DTCP. *JVC 6/24/2004 Ex Parte* at 2.

73.9008 of the Commission's rules.[331]

C. TECHNICAL MATTERS

78. As outlined above, the technology proponents have submitted detailed technical information with their certifications describing the level of security they afford content, how they maintain an appropriate scope of redistribution, their use of authentication, their capacity for revocation, renewal and upgrade, and whether they permit interoperability. Few questions were raised regarding these technical elements; we address any relevant legal and policy issues related to them below.[332] With the sole exception of DTCP over Bluetooth, we are satisfied that, as of the date of this *Order*, each of the output protection technologies and recording methods is technically sufficient in each of these areas to adequately protect digital broadcast television content from indiscriminate redistribution.[333] We recognize nonetheless that technology is ever-evolving, as are the potential threats to security. To the extent that an output protection technology or recording method becomes outmoded or so severely compromised that revocation, renewal or upgrade are insufficient to address the breach, we will consider petitions seeking revocation of our approval pursuant to Section 73.9008(e) of the Commission's rules.[334]

D. LICENSE TERMS

79. Under the Commission's interim process for reviewing output protection technologies and recording methods, we indicated that if a particular technology were to be offered publicly, the technology proponent must submit to the Commission a copy of its licensing terms and fees, in addition to evidence demonstrating that the technology will be licensed on a reasonable, non-discriminatory basis.[335] We further specified that, as part of our application of functional criteria to particular technologies, we would "consider a technology's licensing terms, including its compliance and robustness rules, change provisions, approval procedures for downstream transmission and recording methods, and any relevant license fees."[336] Of the thirteen above-referenced technologies, all except TiVoGuard and the software implementations of MagicGate will be publicly offered.[337]

80. In their oppositions and responses to the twelve licensed technologies, MPAA, Philips, Hewlett Packard, American Antitrust Institute ("AAI") and Genesis Microchip each seek the modification

[331] 47 C.F.R. § 73.9008.

[332] MPAA argued that RealNetworks and Microsoft provided insufficient information regarding their DRM technologies in their certifications. MPAA Opposition to RealNetworks at 2-3, 9; MPAA Opposition to Microsoft at 6. We are satisfied that both parties have supplemented their certifications with adequate information on the technical merits of WMDRM and Helix.

[333] We cannot reach a specific conclusion on the appropriateness of DTCP over Bluetooth in this context since the mapping protocol for this implementation relies upon information contained in the Bluetooth technical specification which has not been submitted by DTLA for Commission review. *See DTLA 6/24/04 Ex Parte* at Attachment. We are therefore unable to approve DTCP over Bluetooth at this time. DTLA may file an amendment to its certification with additional information regarding the Bluetooth technology and we will reevaluate the merits of DTCP over Bluetooth as if it were a new transport. Amendments may be certified pursuant to the procedures outlined in Section 73.9008(c) of the Commission's rules. *See* 47 C.F.R. § 73.9008(c).

[334] 47 C.F.R. § 73.9008(e).

[335] *Broadcast Flag Order*, 18 FCC Rcd at 23575.

[336] *Id*. at 23576.

[337] TiVo does not now and does not intend to offer TiVoGuard as a separate, free-standing digital output protection or recording technology. TiVoGuard Certification at 34. Similarly, Sony intends to keep its software implementations proprietary for its own use and that of its affiliates. MagicGate Memory Stick PRO Software Certification at 2; MagicGate Hi-MD Software Certification at 2.

of certain license terms. We discuss the specifics of their proposals below.[338] As a general proposition, however, we are reluctant to intervene in private industry negotiations. We are nonetheless cognizant of the fact that, by virtue of our adoption of a content protection system for digital broadcast television, we have a responsibility to ensure that our goals are met in a competitively neutral manner that serves the public interest. We believe that we can best accomplish this task through an oversight role in which we largely defer to the private licensing mechanisms established by the technology proponents and their adopters, except in cases of material changes, but provide aggrieved parties with a forum for recourse should these private licensing mechanisms fail. In our discussion of the proposed license modifications below, we articulate certain expectations and presumptions that will inform our oversight role in hopes of providing the technology proponents and their adopters with guidance that will avert potential disputes before they arise.

1. Approval of Downstream Technologies and Interoperability

81. Philips' oppositions to DTCP and CPRM express concern that the assertion of control by DTLA and 4C over the approval of downstream output and recording technologies is unreasonable and anticompetitive.[339] In particular, Philips maintains that these approval mechanisms empower DTLA and 4C to quash competition in so far as they can be used to prohibit DTCP and CPRM-compliant playback devices from using a competing technology to make copies.[340] Philips also anticipates delays in the adoption of new technologies as the result of having to seek what it views as redundant approvals from the Commission and certain technology proponents.[341] AAI raises similar concerns in noting that private contractual arrangements which preserve control over interoperability undermine competition.[342] AAI criticizes the downstream approval mechanisms employed by DTLA and 4C as perpetuating their market power, discouraging entry of non-interoperable products using competitive technologies, and locking consumers into a chain of related products.[343] Philips and AAI dispute any potential technical incompatibility issues and advocate a more open approach where any Commission-approved technology would be permitted downstream.[344]

---

[338] Certain issues raised by MPAA have been resolved through clarifications and commitments made by the certifying entities and therefore do not require Commission action. These issues include: (1) the inapplicability of intellectual property claims and other obligations to non-adopter content providers, broadcasters, and consumers who indirectly trigger approved output protection technologies and recording methods when they embed the flag in content or utilize flag-compliant equipment; and (2) that the founders of specific output protection technologies and recording methods will abide by the same compliance and robustness rules applicable to third party licensees. *See* MPAA Response to Sony at 4-6; MPAA Opposition to Thomson at 11-12; MPAA Opposition to Philips and Hewlett Packard at 5, 8; MPAA Response to DCP at 4-5; MPAA Response to 4C at 3-5; MPAA Opposition to TiVo at 10-11; MPAA Response to DTLA at 5-6; MPAA Opposition to RealNetworks at 11-12; MPAA Opposition to Microsoft at 13-14; MPAA Response to JVC at 3-5; *see also* Sony Reply at 4-6; Thomson Reply at 15; Philips and Hewlett Packard Reply at 7-8, 14-15; DCP Reply at 6; 4C Reply at 7-8; TiVo Reply at 17; DTLA Reply at 5-6; RealNetworks Reply at 11-12; Microsoft Reply at 20-22, 29.

[339] Philips Opposition to DTLA at 21-28; Philips Opposition to 4C at 21-25.

[340] Philips Opposition to DTLA at 22-23, 26-27; Philips Opposition to 4C at 22-23.

[341] Philips Opposition to DTLA at 23-24; Philips Opposition to 4C at 23-24.

[342] AAI Opposition to DTLA at 5; AAI Opposition to 4C at 5; AAI Opposition to DCP at 5.

[343] AAI Opposition to DTLA at 10; AAI Opposition to 4C at 9-10.

[344] Philips proposes that either: (1) DTCP and CPRM's compliance rules be modified to provide that EPN encoded content may be output over, or recorded by, any Commission-approved technology, or (2) that any Commission-approved technologies are deemed approved by DTLA and 4C for use with EPN content. Philips Opposition to DTLA at 24, 27-28; Philips Opposition to 4C at 24-25; AAI Opposition to DTLA at 10; AAI Opposition to 4C at 10.

82. In response, DTLA advocates that the Commission reject any such "automatic" approval requirement out of a concern that DTCP's value would diminish unless DTLA had the ability to ensure effective protection downstream.[345] DTLA suggests that it may be technically infeasible for all output protection technologies and recording methods to interoperate and that unforeseen technical and legal consequences could result from mandated interoperability.[346] From a procedural perspective, DTLA contends that it has worked assiduously with technology proponents and approved every technology that it has reviewed thus far.[347] 4C similarly represents that it has responded promptly to requests for approval of outputs and recording methods, as well as to requests for adapting CPRM to various forms of recordable media.[348]

83. Interoperability is an important pro-competitive element in the consumer electronics and information technology marketplaces that benefits consumers by affording them flexibility to choose among devices made by different manufacturers. We therefore concur with Philips and AAI that interoperability can be a powerful counterbalance where a competitor, or a group of competitors, exercises a significant degree of control in this area. DTCP is in a unique position as one of the two publicly-offered output protection technologies that have been submitted under this interim process, particularly since it is the only such technology that is designed for use with compressed video content and permits copying.[349] DTCP is therefore likely to become the primary output protection technology used in the near term to securely send compressed content between devices. As a result, we must scrutinize any license terms that could constrain competition, such as the downstream approval mechanism questioned by Philips and AAI. We are nonetheless mindful of the technical and practical concerns raised by DTLA relating to interoperability. In order for any two technologies to interoperate, some degree of coordination and harmonization will be needed. We conclude that the license mechanisms used by DTLA and 4C to approve downstream technologies can be useful as forums to facilitate this coordination. Should the proponent of a downstream technology have complaints regarding the implementation of this process, we will consider them pursuant to our general procedures.[350] In approaching any such requests, we will start with the presumption that if an output protection technology or recording method has been approved by the Commission, it should be permitted as a downstream technology where feasible. The upstream technology administrator shall bear the burden of demonstrating in writing, and with specificity, why interoperability is infeasible, whether due to technical incompatibilities, prohibitive costs, or other good cause. We believe that through this oversight role we can minimize any competitive concerns while still affording industry flexibility in determining where

[345] DTLA Reply at 47-50.

[346] *Id*. at 48-49. Examples of these unforeseen consequences include: (1) the fact that certain technologies, like HDCP, are not intended to hand off content downstream; (2) some technologies may not be interoperable at all if a downstream technology requires certain information to be transmitted in the first data stream in order to carry forward any rules or obligations; (3) some technology owners may wish to create closed systems that are not publicly licensed; (4) most technologies require some amount of effort to create interoperability "hooks" between systems, which are issues that should be discussed in the marketplace; and (5) interoperability can present encoding rule issues. *Id*. at 49-50.

[347] *Id*. at 47. DTLA acknowledges that Philips has submitted its Vidi technology for approval as a downstream recording method and that the review process is underway. *Id*. at 48, n.66. DTLA states that Vidi will be treated fairly and thoroughly in due course under this process, as would any other request for approval. *Id*.

[348] 4C Reply at 17. 4C indicates that it is prepared to undertake a prompt review of Vidi and that, if the Commission approves Vidi, and since MPAA has expressed its basic support for the technology, 4C sees no reason why Vidi would not be promptly approved based on currently available information. *Id*. at 17-18.

[349] DTCP and HDCP are also the only content protection technologies that have been approved to date by CableLabs for use with unidirectional digital cable products. *See DFAST Technology License Agreement for Unidirectional Digital Cable Products* at § 2.4 <www.cablelabs.com/udcp/downloads/DFAST_Tech_License.pdf >.

[350] 47 C.F.R. § 1.41.

interoperability can most reasonably be accomplished. We strongly encourage the technology proponents to strive for interoperability wherever possible to ensure that consumers have the widest degree of flexibility when purchasing flag-compliant DTV equipment.

2. Licensing of Intellectual Property

84. As described above, DTCP, HDCP, CPRM, and MagicGate each utilize a necessary claims and reciprocal non-assert approach to licensing intellectual property.[351] Under this approach, the technology proponent agrees not to assert any of its intellectual property claims against adopters if such claims are necessary to manufacture or implement the technology.[352] Adopters in turn must agree not to assert an infringement claim with respect to its own intellectual property against the technology proponent. A number of parties raised concerns regarding aspects of the necessary claims and reciprocal non-assert approach to intellectual property licensing.

85. Genesis Microchip, Inc. ("Genesis") filed an opposition in response to Sony's MagicGate certifications urging that the Commission require the disclosure of any existing or pending patents held by Sony that are necessary to implement the MagicGate technology.[353] In the alternative, Genesis suggests that such patents be disclosed to any prospective adopter upon request.[354] Genesis is concerned that it cannot know whether it holds any patents necessary to implement MagicGate unless it knows the scope of Sony patents that are involved. Thus, Genesis could potentially manufacture a product and later be found liable for patent infringement.

86. Philips opposes the DTCP, HDCP and CPRM necessary claims and reciprocal non-assert provisions on the grounds that they cause barriers to entry that require adopters to forfeit their intellectual property in direct contravention of the Commission's reasonable and nondiscriminatory patent licensing policy.[355] Philips asks the Commission to "recognize the inherent anticompetitive tendency and discriminatory effect of a licensing agreement that requires a licensee to surrender its intellectual property rights against the licensor and against other users of a technology" and which "reduces the incentive to develop innovative new technologies."[356] In response to the CPRM certification, Phillips states that it believes it holds patent rights essential for implementing that technology.[357] Similar concerns are reflected in the comments of Hewlett-Packard regarding the DTCP adopter agreement arguing that the non-assert provision places a potentially large portion of Hewlett-Packard's intellectual property rights in jeopardy.[358] Philips and Hewlett-Packard both advocate an alternative arrangement that permits adopters

[351] *See supra*, ¶¶ 10, 16, 27, 38.

[352] The applicable intellectual property can include, *inter alia*, patents, copyrights, and know-how. *See e.g.*, *Hi-MD Device Hardware Adopter Agreement* at Art. II.

[353] Genesis Opposition to Sony at 2-5. Genesis raised similar arguments in comments filed in the *Digital Broadcast Content Protection* (MB Docket No. 02-230) and *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment* (CS Docket No. 97-80 and PP Docket No. 00-67) proceedings. Petitions for reconsideration in those proceedings are pending.

[354] Genesis Opposition to Sony at 2.

[355] Philips Opposition to DTLA at 6-21; Philips Opposition to DCP at 5-17; Philips Opposition to 4C at 6-21.

[356] Philips Opposition to DTLA at 15, 18; Philips Opposition to DCP at 12, 15; Philips Opposition to 4C at 15, 18.

[357] Philips Opposition to 4C at 12.

[358] Comments of Hewlett-Packard to DTLA at 3-4.

to license any conflicting patents on a reasonable and non-discriminatory basis.[359]

87. AAI[360] urges that the Commission treat the DTCP and CPRM adopter agreements as patent pools and undertake an analysis similar to that used by the Department of Justice in its Business Review Procedure.[361] For purposes of such a review, AAI urges that a patent disclosure requirement be imposed so that a determination can be made as to whether only complementary and essential patents are implicated.[362] AAI also encourages the Commission to evaluate license provisions that AAI regards as competitively harmful, including overly broad reciprocal non-assert provisions that inhibit innovation.[363] Since reciprocal non-assert provisions can provide adopters with disincentive to develop innovations that substitute for necessary claims, AAI believes that "a reciprocal [licensing] obligation that ensures reasonable and non-discriminatory compensation for innovations is self-evidently more pro-competitive."[364]

88. Sony, DTLA, DCP, and 4C rebut these concerns by explaining the rationale underlying their use of a necessary claims and reciprocal non-assert approach.[365] Sony notes that Genesis does not suggest that the necessary claims approach adopted in the MagicGate device hardware agreements is unlawful or fails to satisfy the Commission's interim approval procedures.[366] Sony contends that since content protection is not a feature for which consumers are typically willing to pay, this necessary claims approach allows Sony to offer MagicGate on a cost recovery basis below commercial royalty rates.[367] If Genesis' suggestion were adopted and Sony was required to disclose the specific patent claims covered by the MagicGate specification, Sony indicates that it would be forced to pass on to adopters, and indirectly consumers, the cost of reviewing its patent portfolio.[368] Moreover, Sony argues that it is unclear how the disclosure of intellectual property would even address Genesis' underlying business concern since: (1) the scope of necessary claims would not be fixed until any pending patents were finally issued, and (2) some patents may have both a necessary claims component, as well as some portion that is not required to implement the technology, making the scope of necessary claims difficult to discern.[369]

---

[359] Philips Opposition to DTLA at 5, 21; Philips Opposition to DCP at 4-5, 17; Philips Opposition to 4C at 5, 20-21; Comments of Hewlett-Packard to DTLA at 9.

[360] AAI describes itself as "an independent research, education, and advocacy organization that supports a leading role for competition, as enforced by our antitrust laws, within the national and international economy." AAI Opposition to DCP at 1-2; AAI Opposition to 4C at 2; AAI Opposition to DTLA at 2. Philips and Hewlett-Packard are among AAI's contributors. *See AAI Ex Parte* at Attachment.

[361] AAI Opposition to 4C at 4; AAI Opposition to DTLA at 4.

[362] AAI Opposition to 4C at 4; AAI Opposition to DTLA at 4. Under the Department of Justice guidelines, patent pools involving competing patents are more of a concern than those involving complementary patents. U.S. Department of Justice and Federal Trade Commission, *Antitrust Guidelines for the Licensing of Intellectual Property* at 28-29 (Apr. 6, 1995).

[363] AAI Opposition to DCP at 7; AAI Opposition to 4C at 8-9; AAI Opposition to DTLA at 9. AAI considers such provisions to "favor imitators over innovators." *See* Comments of AAI, MB 02-230 at 2 (filed Feb. 13, 2004).

[364] AAI Opposition to DCP at 6-7; AAI Opposition to 4C at 8-9; AAI Opposition to DTLA at 9.

[365] DTLA Reply at 28-39; DCP Reply at 13-17; 4C Reply at 10-17; Sony Reply at 8-10.

[366] Sony Reply at 7. Sony notes that Genesis' comments are inapplicable to the MagicGate software certifications, which are not publicly licensed. *Id*. at 8.

[367] *Id*. at 8-9.

[368] *Id*. at 9.

[369] *Id*. at 10.

89. In the case of the DTCP adopter agreement, DTLA points out that its terms were also designed to keep the technology's cost low.[370] DTCP was first offered in 1998 to protect a wide range of video content and has since been licensed to more than 75 adopters.[371] DTLA contends that the adopter agreement is pro-competitive in effect and comports with the Commission's traditional meaning in requiring reasonable and non-discriminatory licensing – low cost and equal access.[372] In addition, DTLA maintains that the adopter agreement in no way limits or deters licensees from exploiting their own intellectual property to develop competitive technologies.[373] DTLA suggests that it would be manifestly unfair at this time to change such a fundamental license provision upon which parties have relied since DTCP's inception.[374] Even under a hybrid approach where adopters owning necessary claims were allowed to charge reasonable royalty rates for their patents, DTLA asserts that the 5C Companies would need to start charging commercial royalty rates for their intellectual property.[375]

90. When adopting mandatory technical standards, the Commission's historical focus has been to conduct a sufficient evaluation of the underlying patent rights to prevent any monopoly rights granted under the patent process from being unnecessarily extended through standardization. In other words, the Commission attempts to ensure that no mandatory standard should be so dependent on specific patent rights that the cost of that technology to the public would be adversely affected.[376] The *Broadcast Flag Order* and related Commission rules do not contemplate the adoption of a single federal standard for protecting Marked Content from indiscriminate redistribution. However, a similar concern arises to the extent that the Commission must approve output protection technologies and recording methods for use in this context and that, at least at the beginning of the process, the competitive alternatives may be limited. It is for this reason that Section 73.9008(a)(4) of the Commission's rules require technology proponents to submit their licensing terms for review to ensure that the marketplace and consumers are protected from the imposition of unnecessary costs or anticompetitive constraints.[377]

91. As to the issue of direct costs, our concern that a particular technology will become a *de facto* standard associated with an unreasonable licensing fee has been adequately addressed by the number and variety of technologies we are approving and the prevalence of fee structures based on license administration cost recovery.[378] With respect to the potential for certain license terms to serve as ancillary restraints on competition and technical innovation, the record in this proceeding does not support the Commission's adoption of one approach to intellectual property licensing over another. We agree that particular licensing terms, especially when coupled with market power, could be used in an anticompetitive manner. At this time, we find no evidence has been presented that the necessary claims and reciprocal non-assert approach to intellectual property licensing is *per se* discriminatory, that Sony, DTLA, DCP or 4C has actually engaged in anticompetitive or discriminatory conduct, or that the RAND approach advocated by Philips and Hewlett Packard is inherently preferable in all circumstances. Both approaches are currently used in the marketplace. In reaching this decision, we remain concerned about

[370] DTCP Certification at 17-18 n.8; DTLA Reply at 11-12, 19.

[371] DTCP Certification at 13, 18.

[372] DTLA Reply at 10-20.

[373] *Id*. at 12.

[374] *Id*. at 36-37.

[375] *Id*. at 37.

[376] *See e.g.,* Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service, 6 FCC Rcd 7024, 7034 (1991) (adopting ATSC digital television broadcast standard).

[377] 47 C.F.R. § 73.9008(a)(4).

[378] With respect to D-VHS, there is no evidence on the record that its availability and terms, including pricing, have been unreasonable or discriminatory.

the potential for anticompetitive or discriminatory conduct in this nascent market. As some commenters point out, a particular licensing structure for an approved technology could result in competitors facing difficult choices regarding the protection of their intellectual property and their ability to build devices incorporating that technology which, ultimately, could affect innovation in the market. We believe, however, that our continued oversight, especially concerning the approval of downstream technologies and change management processes in the MagicGate, DTCP, HDCP and CPRM licenses, should effectively curb any potential anticompetitive or discriminatory conduct. In approving the foregoing technologies, the Commission takes no position on the application of the federal antitrust laws to the technology proponents' licensing terms. The Commission reserves the right to reconsider its approvals should a federal court determine that a technology proponent, through its licensing terms or otherwise, violates the federal antitrust laws, or upon a request by the Department of Justice or the Federal Trade Commission on the grounds that a technology proponent's licensing terms raise substantial concerns under the federal antitrust laws. In addition, once flag-compliant devices are introduced in the marketplace, interested parties should: (1) bring concerns to the Commission for appropriate action, (2) bring competitive or antitrust concerns to the attention of the relevant antitrust authorities, or (3) seek private enforcement action in court. At that time, the Commission may revisit the licensing terms of approved technologies.

3. Content Provider Third Party Beneficiary and Enforcement Rights

92. In its oppositions to TiVoGuard, WMDRM and Helix, MPAA seeks its own form of oversight through mandatory third party beneficiary and enforcement rights against manufacturers of downstream devices.[379] MPAA argues that such rights are critical to enforcement of the flag compliance and robustness requirements downstream.[380] TiVo challenges MPAA's request as beyond the Commission's authority and practically unnecessary since TiVo has committed itself and contractually required its downstream device manufacturers to adhere to the Commission's flag compliance and robustness rules.[381] In the event that TiVo or its manufacturers failed to meet these requirements, TiVo suggests that MPAA's members could file a complaint with the Commission or enforce their copyrights privately.[382] RealNetworks and Microsoft take a similar stance.[383] Microsoft additionally cites its commercial relationships with content owners as providing strong incentive to respond to their concerns about security and enforcement, but points to the multi-purpose nature of WMDRM technology and the cross-industry impact of decisions affecting it as reasons why a more formal content owner role is

[379] MPAA Opposition to TiVo at 9; MPAA Opposition to Microsoft at 10; MPAA Opposition to RealNetworks at 10-11. Although MPAA initially questioned the enforcement licensing structure for SmartRight, Thomson's subsequent provision of a content participation agreement in addition to the third party beneficiary rights already contained in the SmartRight adopter agreement have alleviated MPAA's concerns. *See* MPAA Opposition to Thomson at 9-10; Thomson Reply at 11-12, 14; *Thomson 5/28/04 Ex Parte* at 3. MPAA also challenges the inclusion of a € 100 million ($122.8 million) annual revenue threshold for third party beneficiary status to seek injunctive relief under Vidi's adopter agreement. MPAA Opposition to Philips and Hewlett Packard at 7-8. Philips counters that such a threshold is intended to ensure the bona fides of content participants and points to similar requirements in the change management provisions of DTCP's content participant agreement. Philips and Hewlett Packard Reply at 13-14, n.23; *see also* DTCP Certification at Exhibit 3, §§ 1, 3.7(f), 3.8, 3.9(d). Given the presence of similar threshold provisions in other license agreements, we are not inclined to intervene in the negotiation of this specific license term.

[380] MPAA Opposition to TiVo at 9; MPAA Opposition to Microsoft at 10; MPAA Opposition to RealNetworks at 10-11.

[381] TiVo Reply at 12-17.

[382] *Id*. at 15-16.

[383] RealNetworks Reply at 11; Microsoft Reply at 22-27.

impracticable.[384]

93. Although most of the technology proponents have accorded content owners with third party beneficiary and enforcement rights against manufacturers of downstream devices, we are not persuaded that such contractual arrangements should be uniformly mandated. As illustrated by WMDRM, the multi-use nature of certain technologies makes it impracticable for some technology proponents to grant content owners formal enforcement rights which could have significant cross-sector implications. Our expectation is that the commercial relationships between content owners and technology proponents will serve as strong incentive to address potential compliance issues. In addition, we concur with TiVo, Microsoft and RealNetworks that content owners have other enforcement mechanisms available to them, including the ability to appeal to the Commission. Should a technology proponent fail to adequately meet the Commission's flag compliance and robustness rules, whether through their own direct implementation or through contractual relationships with downstream device manufacturers, a content owner may petition the Commission seeking revocation of the technology's approval for use under this order, or other appropriate relief.[385]

4. Change Management

94. Given the dynamic nature of technology today, change management over technical and legal matters is a critical and necessary element both in the administration of the above-referenced output protection technologies and recording methods, as well as the Commission's oversight of this certification process. Opponents have raised concerns regarding change management in two contexts. First, MPAA challenges the change management procedures relevant to Vidi, TiVo, Helix and WMDRM as providing an insufficient role for content owners to object to technical and legal changes.[386] In the absence of a strong content owner role in change management, MPAA advocates that the Commission retain jurisdiction over all changes and should approve any changes before they are implemented.[387]

95. In response, Philips, Hewlett Packard, TiVo, RealNetworks and Microsoft primarily focus on technical changes that may be needed to maintain the security of their technologies. Philips and Hewlett Packard agree that the Commission should retain jurisdiction over all technical changes, except where they are in the nature of bug fixes or the correction of minor errors or omissions.[388] To address content owner concerns, Philips and Hewlett Packard are willing to add a proviso that any such clarifications or corrections shall not have a material and adverse effect on the overall security of Vidi and

[384] Microsoft Reply at 22-26.

[385] 47 C.F.R. §§ 73.9008(e), 76.7; *see also* 47 C.F.R. § 1.41.

[386] MPAA Opposition to Philips and Hewlett Packard at 5-7; MPAA Opposition to TiVo at 10; MPAA Opposition to RealNetworks at 9-10; MPAA Opposition to Microsoft at 11. Just as it had initially challenged the enforcement provisions of the SmartRight adopter agreement, MPAA at first questioned its change management terms, but later acquiesced to new procedures added in the SmartRight content participation agreement. *See* MPAA Opposition to Thomson at 9-10; Thomson Reply at 11-12, 14; *Thomson 5/28/04 Ex Parte* at 3. MPAA also disputes the inclusion of a time limit on arbitration procedures in the Vidi adopter agreement applicable to change management disputes. MPAA Opposition to Philips and Hewlett Packard at 6. Philips counters that the time limit affects a limited scope of permitted changes and will still afford content providers a full and fair opportunity to resolve conflicts since arbitration is only a last resort after all other dispute resolution mechanisms have been exhausted. Philips and Hewlett Packard Reply at 12-13. Given the existence of detailed dispute resolution provisions in the Vidi license, we again defer to the parties to negotiate their specific terms.

[387] MPAA Opposition to Philips and Hewlett Packard at 5-7; MPAA Opposition to TiVo at 10.

[388] Philips and Hewlett Packard Reply at 8. Philips and Hewlett Packard also indicate that the permissible changes relating to broadcast content are very limited under the Vidi license. *Id*. at 9, 11.

that content participants can object to any materially adverse changes.[389] TiVo and RealNetworks emphasize that change management is not required by the Commission's rules.[390] TiVo elaborates that MPAA's request for a formal private role in change management is unnecessary and unreasonable since technology companies have incentive to appropriately handle security changes.[391] TiVo pledges to notify the Commission of any security changes and suggests that if it fails to maintain the security of its system, MPAA can file a complaint with the Commission.[392] Microsoft echoes TiVo in its belief that its commercial relationships provide the business incentives that drive changes to the WMDRM system.[393] Microsoft offers that its Security Advisory Board can serve as a vehicle that allows content owners to provide input on developments affecting the security of WMDRM.[394]

96. The second context in which change management issues are raised relates to the HDCP, CPRM and DTCP licenses. AAI and Philips argue that the change management terms contained in these licenses are overly broad and lack adopter participation.[395] AAI and Philips particularly object to the change management procedures applicable to the HDCP, CPRM and DTCP compliance rules, suggesting that they provide DCP, 4C and DTLA with a competitive advantage through lead time in product design.[396] Philips asserts that the compliance rules applicable to EPN content in the CPRM and DTCP licenses should be those the Commission has adopted in the *Broadcast Flag Order* and any necessary changes should be subject to the process of amending the Commission's rules.[397] With respect to the HDCP compliance rules, Philips proposes that change management be accomplished through an open process with adopter notice and input prior to Commission approval.[398] AAI agrees that any changes other than minor corrections or modifications should necessitate Commission review.[399]

97. DCP responds by saying that there are significant limitations on its practical ability to make changes and assures that it will not knowingly make changes that would render HDCP inconsistent with the Commission's flag compliance and robustness rules.[400] DCP further suggests that, to the extent a technology proponent makes changes that materially affect the technology's compliance with the

[389] Philips and Hewlett Packard Reply at 12.

[390] TiVo Reply at 8; RealNetworks Reply at 10-11.

[391] TiVo Reply at 4-6, 8, 10-11.

[392] *Id*. at 5-6, 8-9.

[393] Microsoft Reply at 24.

[394] *Id*. at 24-25.

[395] AAI Opposition to HDCP at 7; AAI Opposition to CPRM at 9; AAI Opposition to DTCP at 9; Philips Opposition to HDCP at 17-20; Philips Opposition to CPRM at 25-31; Philips Opposition to DTCP at 28-33. In particular, Philips advances that the scope of permissible changes under the DTCP license has been broadly construed by DTLA to include: (1) adding EPN to the encoding rules, (2) limiting personal video recorder ("PVR") copying to 90 minutes, (3) limiting first generation copies to two per format, (4) limiting the number of authorized sink devices from 62 to 34, (5) changing the cipher from M6 to AES, and (5) adding discussions on localization. Philips Opposition to DTCP at 29-30.

[396] *See* AAI Opposition to CPRM at 9; AAI Opposition to DTCP at 9; Philips Opposition to HDCP at 17-20; Philips Opposition to CPRM at 25-31; Philips Opposition to DTCP at 28-33; *see also* Hewlett Packard Comments to DTCP at 5.

[397] Philips Opposition to CPRM at 31; Philips Opposition to DTCP at 33.

[398] Philips Opposition to HDCP at 5, 20. As part of its review and approval of any proposed change, Philips advocates that the Commission take in to account its impact on adopters, the public, and content owners. *Id*.

[399] AAI Opposition to HDCP at 7; AAI Opposition to CPRM at 9; AAI Opposition to DTCP at 9.

[400] DCP Reply at 16-18.

Commission's rules, that technology's approval could be revoked by the Commission.[401] DTLA asserts that not all changes to the DTCP licenses or specifications may be relevant to broadcast protection, and should be of no concern to the Commission.[402] DTLA further submits that permissible changes to the specification must be narrow in scope and that most changes that have occurred derive from porting DTCP to new protocols, something which has only benefited adopters.[403] DTLA also rejects the notion of Commission oversight, whether through advance approval or re-evaluation of changes already made pursuant to change management.[404]

98. As specified with respect to the scope of our approval herein, we are not inclined to grant blanket approvals under which a technology proponent could subsequently make material and substantial changes to their technology or license terms. To do so would undercut the validity of this certification process. At the same time, we do not wish to inhibit innovation or involve the Commission in unnecessary bureaucratic oversight. We will therefore defer to the change management procedures already set in place by the technology proponents for non-material, routine changes to both the technical specifications as well as any applicable license agreements. Included among the changes that we will consider non-material are: (1) bug or minor security fixes; (2) minor errors or omissions; (3) corrections; and (4) routine changes in license fees. To the extent that any party – including content owners, adopters, or others – feel that the change management procedures have been inappropriately invoked or applied, they may file a complaint with the Commission.[405] Where a technology proponent has not established formal change management procedures, it is our expectation that they will consult with content owners and adopters and provide advance notice of any non-material changes as is practicable.

99. Any technical or legal changes that are material and substantial in nature, irrespective of whether a particular technology has formal change management procedures in place, must be submitted to the Commission for approval. Material changes shall include, but are not limited to: (1) mapping to a new transport or media; (2) changes in the encoding or treatment of digital broadcast television content; (3) changes that may have a material and adverse effect on the integrity or security of the technology; (4) changes in the cryptographic method used, except where the algorithm is unchanged and only the key length is expanded; (5) changes in the scope of redistribution; and (6) any fundamental change in the nature of the technology.[406] We will treat any proposed material change as an amendment to the

[401] *Id*. at 17.

[402] DTLA Reply at 54.

[403] *Id*. at 46-47. DTLA counters Philips' characterization of changes that have been made under the DTCP license: (1) adding EPN to the encoding rules benefits consumers by allowing them to copy content; (2) the 90 minute PVR provision for "copy never" content is irrelevant to the instant proceeding, but benefits consumers by guaranteeing a floor to preserve PVR functionality; (3) the limit of 2 copies per format is misleading as a single source can send content simultaneously to 34 sink devices, allowing consumers to make 68 first generation copies in multiple formats of copy once content; (4) the 34 sink device limit was necessary to port DTCP to IP to prevent public networking while preserving the ability to have home and personal networks, but this number can be expanded; (5) the change of cipher is for DTCP-IP and only applies for those adopters that voluntarily decide to implement to DTCP-IP; and (6) adopters have received advance notice that proposed changes for localization may be imposed to reinforce existing obligations, so long as the changes are commercially and technically reasonable so as not to impose material costs on adopters. *Id*. at 50-54.

[404] *Id*. at 6, 54, n.70.

[405] *See* 47 C.F.R. § 1.41.

[406] For example, we will consider the planned merger of WMDRM with Windows Information Rights Management content protection system into one digital rights management system to represent a fundamental change in the nature of WMDRM that merits treatment as a material change. Microsoft Reply at 24, n.22. We will also consider any changes in future releases of WMDRM that materially alter the features, functionality, or compliance and robustness (continued....)

technology proponent's existing certification and will process such amendments on an expedited basis following public notice and comment.[407] When evaluating these amendments, we will not reconsider any issues in the underlying certification that have already been addressed in this *Order,* unless they are directly impacted or modified by the proposed material change. We believe that this oversight role strikes an appropriate balance that will assure the integrity of this certification process while at the same time preserving flexibility for technology proponents in routine management matters and providing content owners and adopters with adequate participation in change management.

5. Revocation and Renewal

100. Revocation and renewal are the primary means by which content protection technologies and recording methods maintain their level of protection in the face of ongoing security challenges. Although several technology proponents indicate that they achieve renewal through revocation,[408] we consider the two processes to be distinct and wish to clarify their meanings. Revocation involves the process of disabling a key so that it can be no longer used for decryption. Depending on the system architecture of a particular technology, revocation can therefore be applied to specific applications or content, individual devices, or a class of devices. Renewal in its true sense refers to the ability of a content protection technology to change its cryptography without hardware or software upgrades.

101. With this distinction in mind, we turn to comments filed by MPAA with respect to the revocation and renewal procedures utilized by TiVo and Microsoft.[409] MPAA questions these procedures in so far as content owners are not given a formal role in initiating revocation or renewal.[410] MPAA specifies that TiVo may have little practical incentive to identify, investigate and take action where revocation and renewal are merited.[411] TiVo counters that a formal private role for content owners is unnecessary and unreasonable since TiVo's business model depends on the security of its system.[412]

(...continued from previous page)
requirements applicable to the protection of digital broadcast content described in Microsoft's certification and subsequent filings in this proceeding to merit treatment as a material change. *See Microsoft 7/13/04 Ex Parte* at 1.

[407] Technology proponents may certify any amendments pursuant to our procedures for subsequent certifications. *See* 47 C.F.R. § 73.9008(c).

[408] *See e.g.*, Vidi Certification at 9; HDCP Certification at 8; CPRM Certification at 9-10 (for products with unique device keys); DTCP Certification at 8-9.

[409] MPAA also raised several issues relating to revocation that were subsequently addressed in reply comments. In its oppositions to SmartRight and Helix, MPAA initially argued that neither Thomson nor RealNetworks had provided adequate information describing their revocation and renewal processes. MPAA Opposition to Thomson at 8-9; MPAA Opposition to RealNetworks at 8. In their replies, Thomson and RealNetworks supplied additional detail. Thomson Reply at 12-13; RealNetworks Reply at 8-10. Thomson also accorded content participant agreement signatories with a formal role in revocation and renewal procedures. Thomson Reply at 12-13. In its response to Sony's MagicGate technologies, MPAA sought clarification that all 300 MB HiMD recorder devices and software are subject to revocation. MPAA Response to Sony at 5. Sony confirmed in its reply that all MagicGate HiMD products, both hardware and software, must be capable of the same revocation process as its 1 GB media. Sony Reply at 5.

[410] MPAA Opposition to TiVo at 8; MPAA Opposition to Microsoft at 9. MPAA also seeks clarification on Microsoft's delivery of revocation and renewal information, particularly with respect to hardware implementations. MPAA Opposition to Microsoft at 9. Microsoft elaborates that the delivery of revocation information is handled through as many mechanisms as possible, while renewal information is propagated through WMDRM-protected content in Internet and physical media. Microsoft Reply at 15-18. Microsoft pledges to seek out additional delivery mechanisms. *Id*. at 17-18.

[411] MPAA Opposition to TiVo at 8.

[412] TiVo Reply at 4, 6-7.

TiVo welcomes information from content owners and others about potential security compromises, but feels that adding an additional layer of private contractual negotiations would be time consuming and add little to reinforce content protection.[413] In a similar vein, Microsoft stresses that content owners generally have the ability to provide input on revocation matters through its Security Advisory Board and that certain *pro forma* responses to security breaches have been negotiated with specific content owners.[414] Given the multi-purpose nature of its WMDRM technology and the cross-sector impact of revocation and renewal decisions affecting it, Microsoft submits that there must be limits on the scope of decision-making authority afforded to content owners.[415] We are persuaded that TiVo and Microsoft have sufficient business incentive to properly implement revocation and renewal where warranted, but nonetheless encourage their continued collaboration with content owners on such matters. To the extent that TiVo or Microsoft fails to address revocation and renewal concerns, content owners may petition the Commission under our general procedures or take private enforcement action.[416]

102. MPAA's oppositions and responses with respect to each technology also contain global comments regarding the potential use of the ATSC transport stream to transmit revocation and renewal data.[417] MPAA perceives a need for a standardized means of delivering this data in the ATSC transport stream and queries the technology proponents on how such information would be received, processed and conveyed.[418] Sony reiterates that revocation information is exchanged and propagated among its MagicGate hardware and software products through media, rendering unnecessary the delivery of revocation information through other means.[419] TiVo likewise asserts that its system, which automatically revokes devices that do not communicate with TiVo's central server, adequately addresses any revocation concerns.[420] Other technology proponents, such as Thomson, Philips, Hewlett Packard, DCP, 4C, RealNetworks, Microsoft and JVC, express a willingness to work with content owners and other stakeholders to develop a standardized means of delivering revocation and renewal information through the ATSC transport stream.[421]

103. Our analysis of the above-referenced output protection technologies and recording methods reflects that each currently has in place appropriate mechanisms to disseminate revocation and renewal information. To the extent that industry wishes to explore new avenues for the delivery of such information, we encourage them to do so and to consult with all affected parties and we will monitor their progress. We must nonetheless express significant concerns regarding the potential use of the public airwaves to transmit data that could limit the functionality of consumer devices or possibly turn them off.

---

[413] *Id*. at 7, 10-11.

[414] Microsoft Reply at 24-25.

[415] *Id*. at 25-26.

[416] *See* 47 C.F.R. § 1.41.

[417] MPAA Response to Sony at 6; MPAA Opposition to Thomson at 9; MPAA Response to Philips and HP at 8; MPAA Response to DCP at 5; MPAA Response to 4C at 5; MPAA Opposition to TiVo at 8-9; MPAA Response to DTLA at 6; MPAA Opposition to RealNetworks at 9; MPAA Opposition to Microsoft at 10; MPAA Response to JVC at 5-6.

[418] MPAA Response to Sony at 6; MPAA Opposition to Thomson at 9; MPAA Response to Philips and HP at 8; MPAA Response to DCP at 5; MPAA Response to 4C at 5; MPAA Opposition to TiVo at 8-9; MPAA Response to DTLA at 6; MPAA Opposition to RealNetworks at 9; MPAA Opposition to Microsoft at 10; MPAA Response to JVC at 5-6.

[419] Sony Reply at 6.

[420] TiVo Reply at 7-8.

[421] Thomson Reply at 13-14; Philips and Hewlett Packard Reply at 15-16; DCP Reply at 7; 4C Reply at 9; RealNetworks Reply at 9; Microsoft Reply at 17-18; JVC Reply at 6.

Indeed, we have similar concerns about the potential use of the ATSC transport stream to transmit any content protection information beyond that which was specifically approved in the *Broadcast Flag Order*.[422] Industry should advise and consult with the Commission before it implements any new uses of the ATSC transport stream to deliver content protection information.

6. Compliance and Robustness

104. Apart from the change management issues discussed above, compliance and robustness matters have been raised in two limited contexts. MPAA questions TiVo and Microsoft regarding the compliance and robustness rules applicable to downstream devices incorporating TiVoGuard and WMDRM.[423] Since TiVoGuard will not be publicly licensed, MPAA seeks assurance from TiVo that any downstream devices will abide by the Commission's flag compliance and robustness rules.[424] TiVo affirms that it will adhere to the Commission's flag compliance and robustness rules with respect to any downstream device it manufactures, sells or distributes and will contractually obligate downstream product manufacturers to do the same.[425] In the case of Microsoft, MPAA challenges the adequacy of its compliance and robustness rules and the means by which they will be applied downstream.[426] Microsoft explains that since it does not currently license WMDRM for third party implementations, it has no need to formalize and publish its internal robustness requirements.[427] Given its future plans to license such implementations, however, Microsoft states that it has developed a set of applicable compliance and robustness rules for its network streaming and USB connected storage device implementations, and is in the process of developing similar compliance rules governing the transfer of content over IP among connected storage devices.[428] We conclude that both TiVo and Microsoft have instituted sufficient compliance and robustness requirements for downstream devices incorporating the TiVoGuard and WMDRM technologies, but condition our approval of the WMDRM implementation permitting the transfer of content over IP on Microsoft submitting to the Commission the final compliance rules applicable to this implementation.

7. Associated Obligations

105. A final area touched upon in several of MPAA's oppositions and responses involves upstream controls over downstream HDCP functions.[429] In order for HDCP to function properly, certain actions need to be taken by a Covered Demodulator Product prior to delivering content to the HDCP

[422] In the *Broadcast Flag Order*, we specified that "to the extent broadcasters wish to use the ATSC flag to protect unencrypted DTV broadcasts, they may do so provided they do not transmit the optional additional bits provided for in ATSC A/65B." *Broadcast Flag Order,* 18 FCC Rcd at 23569.

[423] MPAA also seeks clarification from Sony that the same robustness requirements applicable to hardware implementations of its MagicGate technology will similarly govern its software implementations. MPAA Response to Sony at 5. In its reply, Sony confirms that Section 12.1 of its content participant agreement for MagicGate requires its software and hardware implementations to abide by the same robustness rules. Sony Reply at 4-5.

[424] MPAA Opposition to TiVo at 7.

[425] TiVo Reply at 3-4.

[426] MPAA Opposition to Microsoft at 7-8.

[427] Microsoft Reply at 19-22.

[428] *Microsoft 5/18/04 Ex Parte* at 1-2; *Microsoft 6/25/04 Ex Parte* at Attachments; *Microsoft 7/28/04 Ex Parte* at n.3. In addition, Microsoft has formalized a set of compliance rules that will govern Microsoft's implementation of WMDRM in Windows, which will not be licensed for third party implementation. *Microsoft 5/18/04 Ex Parte* at 1-2.

[429] MPAA Response to Sony at 3-4; MPAA Opposition to Thomson at 7-8; MPAA Response to Philips and HP at 3-4; MPAA Response to DCP at 3-4; MPAA Response to DTLA at 4-5; MPAA Response to JVC at 5-6.

output.[430] DCP describes these "associated obligations" as ensuring that an HDCP source function is fully engaged, with its encryption active, before delivering protected content to the output.[431] The associated obligations outlined by DCP also require Covered Demodulator Products to deliver and process any SRMs that might be included in content for revocation purposes.[432] MPAA seeks to impose these associated obligations through the adopter agreements applicable to output protection technologies or recording methods.[433] For example, if Sony authorized HDCP as a protected downstream output, MPAA would have the MagicGate device hardware adopter agreements require compliant Covered Demodulator Products to assert upstream control of the flow of content being sent to an HDCP function.[434]

106. Sony responds by suggesting that any associated obligations are more appropriate as part of the Commission's rules than as part of the MagicGate license, but acknowledges that a similar obligation is already contained in its compliance rules.[435] In contrast, Thomson, Philips, and Hewlett-Packard believe that the best resolution is for DCP to change the HDCP specification or compliance rules.[436] DCP objects, noting that these associated obligations "are 'upstream' from the HDCP output, and thus, not covered by the HDCP license obligations."[437] DCP joins DTLA and JVC in advocating that the Commission require Covered Demodulator Products to comply as a condition of HDCP's approval under this certification process.[438] DTLA asks that similar associated obligations relating to DTCP be adopted to ensure SRMs are delivered and processed, and to set the appropriate data fields to signal EPN encoding.[439]

107. In establishing our compliance rules for Unscreened and Marked Content, we recognized that additional technical requirements specific to a particular Authorized Digital Output Protection Technology might be needed to ensure that when Covered Demodulator Products send content to outputs protected with such technology, they function correctly.[440] It is for this reason that we expressly provided that Unscreened and Marked Content could be sent "to a digital output protected by an Authorized Digital Output Protection Technology, *in accordance with any applicable obligations established as a part of its approval pursuant to [Section] 73.9008*."[441] It is incumbent on manufacturers of Covered Demodulator Products using HDCP or DTCP-protected outputs to ensure that these output protection technologies function correctly. As a condition of our approval of HDCP, we therefore expect that manufacturers of Covered Demodulator Products will verify that the HDCP source function is fully engaged and able to deliver protected content, meaning that HDCP encryption is operational on such output. For DTCP, we expect that Covered Demodulator Product manufacturers will appropriately set the needed data fields to

[430] *DCP 6/25/04 Ex Parte* at 3.

[431] HDCP Certification at 15; DCP Reply at 5-6.

[432] HDCP Certification at 15; DCP Reply at 5-6.

[433] MPAA Response to Sony at 3-4; MPAA Opposition to Thomson at 7-8; MPAA Response to Philips and HP at 3-4; MPAA Response to DTLA at 4-5; MPAA Response to JVC at 5-6.

[434] MPAA Response to Sony at 3-4.

[435] Sony Reply at 2-4.

[436] Thomson Reply at 10-11; Philips and HP Reply at 5-6.

[437] *DCP 6/25/04 Ex Parte* at 3.

[438] HDCP Certification at 15; DCP Reply at 5-6; DTLA Reply at 5; JVC Reply at 4.

[439] DTLA Reply at 4-5.

[440] 47 C.F.R. §§ 73.9003(a)(3), 73.9004(a)(3).

[441] *Id*. (emphasis added).

indicate EPN encoding.[442] We are not persuaded, however, that obligations relating to SRMs delivered in content are needed at this time, given the lack of a standard for delivering revocation information in the ATSC transmission stream.[443] To the extent that such a standard is developed, and we determine that the delivery of revocation data in this manner is an appropriate use of the public airwaves, we may revisit this issue at that time. Since a number of alternative mechanisms exist to deliver and propagate revocation information, we do not believe that the ability of technology proponents to revoke compromised devices or components will be disadvantaged in the interim.

IV. ORDERING CLAUSES

108. **IT IS ORDERED** that pursuant to the authority contained in Sections 1, 2, 4(i) and (j), 303, 307, 309(j), 336, 337, 396(k), 403, 601, 614(b) and 624a of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i) and (j), 303, 307, 309(j), 336, 337, 396(k), 403, 521, 534(b) and 544a, the above-captioned digital output protection technologies and recording methods **ARE APPROVED** pursuant to Section 73.9008 of the Commission's Rules, to the extent described herein.

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch
Secretary

[442] Manufacturers should set the following fields of the DTCP Descriptor to the indicated binary values: APS: 00 (copy-free), DTCP_CCI: 00 (copy-free), EPN: 0 (EPN-asserted), Image_Constraint_Token: 1 (not constrained), Retention_State: 000 (forever). Capitalized terms have the same meaning as set forth in the DTCP specification and adopter agreement.

[443] *See supra*, ¶¶ 102-103.

STATEMENT OF
COMMISSIONER KEVIN J. MARTIN
APPROVING IN PART AND CONCURRING IN PART

Re: Digital Output Protection Technology and Recording Method Certifications, Order (August 4, 2004)

I support this Order's approval of over a dozen technologies for use in digital television equipment to give effect to the "broadcast flag."

I write separately to express my concern with two issues. First, I fear that the "non-assert" clause in the DTCP adopter agreement could hinder competition and suppress innovation. We acknowledge in the Order that DTCP is the only publicly-offered output protection technology we approve that permits copying, and is "therefore likely to become the primary" standard for the foreseeable future. As a result, anyone who wants to build products for this market must sign the DTCP license. Yet, the license requires that companies give up any intellectual property rights they have in the DTCP technology before signing. Therefore a party may have to choose between the lesser of two evils: either don't participate in the relevant product market, or compete, but give up your intellectual property rights. I am concerned this result may be anti-competitive, may discourage future investment in intellectual property, and may generally be counter to good public policy.

Second, I am concerned that Tivo's technology does not include sufficient constraints. All of the other technologies requesting approval from us have adopted proximity controls or similar mechanisms to limit content redistribution outside the home at this time. I ultimately want to enable a person's digital networking environment to extend beyond the home. I fear, however, that we may be acting prematurely in concluding that Tivo's affinity controls are sufficient to protect against widespread redistribution. I therefore would have conditioned approval of Tivo's technology on adoption of proximity controls at this time, and continued to study whether its device limits and affinity controls provide adequate protection.