

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

In the Matter of)	
)	
Video Device Competition)	MB Docket No. 10-91
)	
Implementation of Section 304 of the Telecommunications Act of 1996)	
)	CS Docket No. 97-80
Commercial Availability of Navigation Devices)	
)	
Compatibility Between Cable Systems and Consumer Electronics Equipment)	PP Docket No. 00-67
)	

To: The Commission

COMMENTS OF NAGRAVISION

Robin Wilson
Vice President, Business Development
Nagravision
841 Apollo St.
El Segundo, CA 90245
robin.wilson@nagra.com

July 13, 2010

TABLE OF CONTENTS

SUMMARY AND INTRODUCTION iii

I. STRUCTURAL PROBLEMS SHOULD BE ADDRESSED2

 A. Simulcrypt Interfaces Will Enable Competition Among Conditional Access Vendors 3

 B. Breaking the Lock between Conditional Access and Set-Top Box Vendors Will Encourage Competition 5

 C. Independent Third Party Certificate Issuance and Certification Will Facilitate Competition..... 7

II. DTCP-IP IS NOT A COMPLETE SOLUTION FOR ALLVID NETWORKS.....7

 A. DTCP-IP is Designed for a More Narrow Application Than Needed for an AllVid Network..... 8

 B. DTCP-IP Security Concerns 10

III. INTELLECTUAL PROPERTY10

IV. DOWNLOADABLE SECURITY ISSUES ARE ORTHOGONAL TO THE ALLVID DISCUSSION11

V. USER INTERFACES SHOULD BE UNENCUMBERED12

CONCLUSION.....14

SUMMARY AND INTRODUCTION

Nagravision, a Kudelski Group company, is the leading supplier of open conditional access systems (“CAS”), digital rights management (“DRM”) and integrated on-demand solutions for content providers and digital TV operators over broadcast, broadband and mobile platforms.

In these Comments, Nagravision describes structural problems in the marketplace which the Commission should address in order to allow a competitive environment to develop. We also describe areas of security that DTCP-IP does not address, and other issues including intellectual property, downloadable security and user interfaces.

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

In the Matter of)	
)	
Video Device Competition)	MB Docket No. 10-91
)	
Implementation of Section 304 of the Telecommunications Act of 1996)	CS Docket No. 97-80
)	
Commercial Availability of Navigation Devices)	
)	
Compatibility Between Cable Systems and Consumer Electronics Equipment)	PP Docket No. 00-67
)	

To: The Commission

COMMENTS OF NAGRAVISION

Nagravision, a Kudelski Group company, is the leading supplier of *open* conditional access systems (“CAS”), digital rights management (“DRM”) and integrated on-demand solutions for content providers and digital TV operators over broadcast, broadband and mobile platforms.¹

Nagravision hereby respectfully submits these comments in response to the Commission’s Notice of Inquiry seeking comments on specific steps that can be taken to unleash competition in the retail market for smart, set-top video devices (“smart video devices”) that are

¹ Nagravision is a division of the Kudelski Group, a publicly traded company based in Switzerland. Its technologies are currently being used by more than 120 leading Pay-TV operators worldwide securing content delivered to over 124 million active smart cards and devices, and more than 14 million households served by MPVDs in the United States.

compatible with all multichannel video programming distributor (“MVPD”) services.² In these comments, we stress the importance of:

- i) Enabling competition among CAS and DRM providers as another source of innovation;
- ii) Supporting the broad set of evolving services that MVPDs are offering consumers while maintaining a high level of service and content protection;
- iii) Ensuring a fair IP regime in any mandated system;
- iv) The orthogonality of the issue of downloadable security to the AllVid discussion; and
- v) Unrestricted electronic program guides for bringing innovation to consumers.

I. STRUCTURAL PROBLEMS SHOULD BE ADDRESSED

The Commission should keep in mind that the failure of CableCARD was a business failure, not a technical failure. The business failure was not due to costs or consumer demand; it was instead due to fundamental structural issues in the marketplace.

A device very similar to the CableCARD, i.e., the DVB-CI+ module,³ is becoming very successful in Europe, and not coincidentally is doing so by avoiding many of the pitfalls that befell the CableCARD. CI+ modules are similar in cost to CableCARDs and costs to implement the slot on retail devices are similar to CableCARD costs. Module costs are not an issue, and European consumers are willing to purchase CI+-capable TV’s, just as U.S. consumers were willing to purchase CableCARD-capable televisions.

Factors beyond cost and consumer demand are enabling CI+ to be successful, where CableCARD fails. The factors inhibiting success in the U.S. marketplace are structural and the Commission must deal with them or any attempt at implementing Section 629 will likely fail.

² *Video Device Competition; Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Notice of Inquiry, MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67, 25 FCC Rcd 4275, 75 FR 27264 (2010) (“Notice”).

³ See www.ci-plus.com.

There are three main structural issues which the Commission should address. First, there must be real competition between conditional access vendors. Second, there must be a competitive market to supply set-top boxes to MVPDs (unconstrained by conditional access systems). Third, certification testing and key and certificate issuance must be established and operated by an independent third-party.

A. SIMULCRYPT INTERFACES WILL ENABLE COMPETITION AMONG CONDITIONAL ACCESS VENDORS

In the United States, there are effectively only two Conditional Access (“CA”) vendors in cable (with more than 90% market share between them), and each of them is also the set-top box vendor. If a cable operator wanted to convert to a competing system, they would face the nearly insurmountable problem of needing to replace nearly all of their capital equipment to effect the change.

Simulcrypt is a system that allows one or more conditional access systems to operate simultaneously on the same system.⁴ This approach successfully undermines “vendor lock” by allowing multiple suppliers of set-top boxes or gateway devices to be able to partner with multiple suppliers (actual or potential) of network-compatible conditional access systems to address the needs of a particular system operator.⁵ This has been shown to create competition in regions where deployed. Simulcrypt has been mandated in almost all parts of the world (e.g., throughout the European Union, South America and in China), either directly or effectively by

⁴ ETSI TS 101 197 v1.2.1, *DVB SimulCrypt; Part 1: Head-End Architecture and Synchronization* (Feb. 2002), available at www.etsi.org/deliver/etsi_ts/101100_101199/101197/01.02.01_60/ts_101197v010201p.pdf; ETSI TS 103 197 v1.5.1, *Head-End Implementation of SimulCrypt* (Oct. 2008), available at www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf; ETSI TS 102 035 v1.1.1, *Implementation Guidelines of the DVB Simulcrypt Standard* (Feb. 2004), available at www.etsi.org/deliver/etsi_tr/102000_102099/102035/01.01.01_60/tr_102035v010101p.pdf.

⁵ “Vendor lock” is where the two primary suppliers of content protection are able to control and license their technology in such a way that true competition is avoided. This is sometimes also referred to as a “CA Duopoly”.

defining a common scrambling system (thereby enabling Simulcrypt).⁶ It is also part of the Advanced Television Systems Committee (“ATSC”) standard⁷ and is used in DBS in the United States. It should be noted that Simulcrypt does not actually have to be used to satisfactorily perform the function of encouraging competition – its *mere presence* is usually enough to discourage anti-competitive behavior, as there is no longer vendor lock.

However, Simulcrypt has never been mandated (nor significantly deployed) in cable systems in the United States.⁸ Instead, the CableCARD system attempted unsuccessfully to avoid common scrambling by locating the proprietary scrambling algorithm in the CableCARD.⁹ Even if the scrambling system used is common and standardized, the Motorola/Cisco duopoly still controls the secret keys that are necessary for the system to function.¹⁰ Thus instead of addressing the root cause of vendor lock, the CableCARD system simply tried to side-step it

⁶ Council Directive 95/47/EC has the effect of requiring DVB Simulcrypt in the European Union, *see* Council Directive No. 95/47/EC, O.J. L. 281/51 (1995); “Italian regulation requires access to conditional access systems (CAS) on fair, reasonable and non-discriminatory terms for third parties and contains simulcrypt [sic] obligations”, Comm’n Decision No. 2004/311/EC, O.J. L. 110/90 at 104 (2004); *see generally* Press Release, Irdeto, *Irdeto Selected to Protection Content & Business Model Protection to Chinese Cable Networks in Hebei and Xinjiang, Over Two Million Smartcards to be Deployed* (June 24, 2008), available at <http://www.irdeto.com/press/55.html> (announcing selection of Irdeto simulcrypt systems for deployment in China).

⁷ *See* ATSC A/70A, *Conditional Access System for Terrestrial Broadcast, Revision A, with Amendment No. 1* (Sep. 2006), available at <http://atsc.org/cms/index.php/standards/published-standards/55-atsc-a70-standard>.

⁸ *But see* Leslie Ellis, *To Seal In Revenues, Open the Video Lock*, Multichannel News (Mar. 17, 2002), available at http://www.multichannel.com/article/70775-To_Seal_In_Revenues_Open_the_Video_Lock.php (indicating that as of 2002, Simulcrypt had been implemented in several cable systems). Nevertheless, openness and standardization has been prevented, *see supra* note 9.

⁹ Scrambling algorithms in US cable are apparently standardized, but without some additional and closely held secret information, the standards are cryptographically locked to specific suppliers.

¹⁰ Comments of TiVo, Inc., GN Docket Nos. 09-47, 09-51, 09-137, CS Docket No. 97-80 (Dec. 22, 2009) at 2.

while simultaneously entangling it with the already complex initiative over the navigation functions.

The Commission should note that Nagravision is not alone in calling for implementation of Simulcrypt interfaces in the United States as a mechanism to increase competition in the market for both set-top boxes and headend equipment.¹¹

Even in the IPTV marketplace we have seen evidence that the marketplace for IPTV distribution equipment is beginning to see equipment and systems that are cryptographically locked and would limit competition.

Section 629 instructs the Commission to “... in consultation with appropriate industry-setting organizations ... assure the commercial availability” of navigation devices.¹² *The Commission should take bold new action to eliminate vendor lock, in part by mandating interoperable conditional access systems via Simulcrypt interfaces. Such a mandate need not make existing systems obsolete, but would increase competition, decrease costs and increase innovation and features throughout the MVPD networks.*

B. BREAKING THE LOCK BETWEEN CONDITIONAL ACCESS AND SET-TOP BOX VENDORS WILL ENCOURAGE COMPETITION

As discussed above, one of the marketplace features that doomed the CableCARD system to failure – and locks cable operators into one vendor, without any real opportunity to switch – is the fact that the conditional access vendor and the set-top box vendor are identical. Any solution

¹¹ Comments of the American Cable Ass’n, GN Docket Nos. 09-47, 09-51, 09-137, CS Docket No. 97-80 (filed Dec. 21, 2009) at p.4 (“The Motorola and Cisco/Scientific Atlanta set top box duopoly presents a significant barrier to the development of a competitive marketplace for set top boxes”); Letter from Mark J. Palchick, Counsel to Massillon Cable Communications Inc., to Marlene H. Dortch, Secretary, Federal Communications Comm’n, Sept. 17, 2009, CS Docket No. 97-80, at p1 (“... the absence of SimulCrypt technology in Motorola and Cisco headends may be artificially limiting competition for price and features among set top boxes”); Letter from Robert Gessner, President, Massillon Cable TV, Inc., to Marlene H. Dortch, Secretary, Federal Communications Comm’n, Aug. 21, 2009, CS Docket No. 97-80, at p. 2 (“Cable providers need access to (and support for) a system known as SimulCrypt in order to preserve the benefits of low-cost set-top converters ...”) (emphasis in the original, internal citations omitted).

¹² 47 U.S.C. § 549(a).

that creates a competitive marketplace for navigation devices must deal with this existing anti-competitive environment.

We discuss above how Simulcrypt may address vendor lock and monopolistic practices from a technology perspective. However, there may be a more direct way of opening networks to competitive navigation devices. As discussed above, cable system architectures in the United States result in a vendor lock situation. While alternative CE suppliers are licensed, these are under the terms negotiated by a competitor who has absolute control over the licensing (or lack thereof) on the mandatory content protection technology.¹³

For many years, the Commission has proceeded under a theory that promulgating regulation that allows mere *attachment* of navigation devices was sufficient to satisfy the goals of Section 629.¹⁴ However, as we note above and others have noted repeatedly, mere attachment does not guarantee full operation – at least partially because of the vendor lock situation described above.

We urge the Commission to consider whether imposing a ban such that no single company may supply both set-top boxes or gateway devices and conditional access. We believe this would be a more successful way to effect real competition. For example, similar initiatives have prevented companies from supplying web browsers tied to operating systems.¹⁵ In the case of set-top boxes and conditional access systems, the potential for locks is more insidious. In this

¹³ See generally CableLabs, <tru2way> *HOST DEVICE LICENSE AGREEMENT*, available at http://www.opencable.com/downloads/tru2way_agreement.pdf (Aug. 26, 2009) (requiring all devices be tested and certified by CableLabs; requiring that host devices implement both a “CE Mode” and “Cable Mode”, prohibiting innovations which mix cable operator-supplied and other content).

¹⁴ See *In The Matter of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, Report and Order, FCC 98-116 at 28 (Rel. June 24, 1998).

¹⁵ See generally *United States v. Microsoft Corp.*, 253 F.3d 34, 259 (D.C.Cir. 2001) (describing unlawful tying of Internet Explorer to Windows 95 and Windows 98 in violation of the Sherman Act).

case, the set-top box can be cryptographically locked to the conditional access system – in other words, without disclosure of the secrets, no other entity will ever be able to access the market.

Finally, should the Commission adopt network agnostic gateway regulations, it should take advantage of the “clean sheet” opportunity to prohibit operators from deploying both gateway devices and conditional access systems that are manufactured by a single supplier. This would have the desired effect of creating opportunities for various suppliers and manufacturers to compete and innovate without anti-competitive pressures.

C. INDEPENDENT THIRD PARTY CERTIFICATE ISSUANCE AND CERTIFICATION WILL FACILITATE COMPETITION

As the Commission has noted in the National Broadband Plan and the Fourth Further Notice, there have been obstacles in the process for certification of CableCARD devices. The Fourth Further Notice proposes rules which could address some of the symptoms of the problems, but does not go far enough.

Under the present CableCARD regime, Cable Television Laboratories (“CableLabs”) is the sole licensor of mandatory technology, the sole tester of “first” devices, the sole approver of all devices, and the source of necessary cryptographic certificates.

For AllVid, or any implementation of Section 629, to succeed, an independent third party should be established and entrusted with certification of devices, licensing of any necessary gating technology,¹⁶ and issuance of cryptographic certificates.

II. DTCP-IP IS NOT A COMPLETE SOLUTION FOR ALLVID NETWORKS

Any network intended to interconnect MVPD adaptors and consumer electronics equipment must have the means to pass not only all of the audio-visual content and metadata required in its full resolution and breadth, but must also support a rich set of usage rights that are

¹⁶ In the CableCARD system, a license for “DFAST” is required. DFAST is a component of the copy protection scheme between the CableCARD and the host device, and CableLabs licenses DFAST to retail device manufacturers. We do not anticipate that DFAST is necessary in an AllVid system, but if there is a necessary licensing regime, it should be developed and administered by an independent third party.

used to create the various offers to consumers today, plus include extensibility for the future. The content and metadata must also be secured to protect the very business models of the content owners, MVPDs and manufacturers that include such capabilities in their products. DTCP-IP does not fulfill these requirements.

A. DTCP-IP IS DESIGNED FOR A MORE NARROW APPLICATION THAN NEEDED FOR AN ALLVID NETWORK

The Commission seeks comments on encryption and authentication of the AllVid network that interconnects the various devices in the home. The Commission states that it believes that the DTCP-IP standard would be a logical choice for content encryption and device authentication. This technology was indeed approved by CableLabs, under the impetus of letters from four studios, and it is the mandatory link protection mechanism for DLNA.¹⁷

While DTCP-IP is a good link protection technology, it is not a DRM. Link protection technologies, like DTCP, protect content as it passes between two trusted devices that are bound by the terms of a license. It relies heavily on the robustness of the devices at the end points of the link since the content is available to them in unprotected form. DTCP has a *very* limited set of usage rules available to it: “copy-free”, “copy-one-generation”, “no-more-copies” or “copy-never”.¹⁸ It can also enable the pausing of content. As implemented under the DLNA guidelines, DTCP-IP is specified only for “display-only” use, enabling a networked display to receive streaming video from a DLNA source.

Compare the “display-only” scenario to the use cases commonly available to customers of MVPDs today. It is common practice to rent movies for a limited time, for example, both in brick-and-mortar contexts and digitally. Often pay-per-view content is sold for a 24-hour

¹⁷ *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices, Compatibility Between Cable Systems and Consumer Electronics Equipment*, Comments of the Digital Living Network Alliance, CS Docket No. 97-80, PP Docket No. 00-67 (June 14, 2010) at 4.

¹⁸ See Hitachi, Ltd, *et al.*, *Digital Transmission Content Protection Specification, Volume 1 (Informational Version)*, Rev. 1.6 (Mar. 19, 2010) at 40 available at http://www.dtcp.com/documents/dtcp/Info_20100319_DTCP_V1_1p6.pdf (describing the four possible values for the two EMI bits).

viewing period. There are many different rights capabilities and permutations that have been used for distribution of content.¹⁹ Recently, many MVPDs are offering the ability to enjoy content received on one device, like a set-top box or a digital video recorder, to be available on other devices like PCs and mobile phones. DTCP lacks the ability to support these services to consumers. Moreover, DTCP does *not* have the capability to signal even content security aspects that the Commission had considered for years and recently granted: selectable output control.²⁰ At present, content that is sent to DTCP compliant devices may be sent to analog outputs.

Modern conditional access systems and DRM systems used by MVPDs and over-the-top Internet-based service providers have sophisticated rights expression technologies developed in response to the content owners' and service providers drive to meet varying and evolving consumer demands. Any AllVid network security solution must support the breadth of services currently offered and must not be an inhibitor to innovation in the future to meet consumer demands.

Because DTCP-IP is only a link protection system with limited usage models further constrained to display-only by DLNA, it does not provide sufficient security or flexibility to meet the needs of an AllVid system. DTCP-IP, by itself does not provide even the level of DRM functionality necessary today, and is certainly not future-proof.

This is a gaping hole that must necessarily be filled before any successful attempt to define an AllVid solution. For some of our customers NagraVision has developed an alternative to DTCP-IP that resolves our concerns over DTCP-IP.

¹⁹ Various rights capabilities, permutations and restrictions include the four DTCP-signaled rights, *id.*, as well as region coding, image constraints (“downresolution”), and selectable output control.

²⁰ See *Motion Picture Ass’n of Am.; Pet. for Expedited Special Relief; Pet. for Waiver of the Comm’n’s Prohibition on the Use of Selectable Output Control* (47 C.F.R. § 76.1903), Memorandum Opinion and Order, CSR-7947-Z, MB Docket No. 08-82, 25 FCC Rcd 4799 (May 7, 2010).

B. DTCP-IP SECURITY CONCERNS

Generally, security mechanisms are audited by independent bodies for robustness, to determine if the technologies are sufficiently secure and robust for the intended use. This is generally required by studios, operators and others with a stake in the security of the technology. While these audit reports are generally very confidential documents, summaries of the results may be made available without compromising security.

We are not aware of such audit summaries for DTCP implementations. We suggest that audit summaries should be made available that describe the security and robustness of the DTCP-IP certificate. Similarly, audit summaries should be made available that summarizes an audit of the compliance of consumer electronics devices to the DTCP requirements.

Absent publicly available security audit summaries, we have concerns that DTCP implementations may not be as secure as they need to be.

III. INTELLECTUAL PROPERTY

The Commission seeks comment on intellectual property issues related to proposed standards for the AllVid adapter, and in particular, should a requirement for reasonable and nondiscriminatory (“RAND”) licensing terms for AllVid-related standards be required.²¹

A requirement for licensing under RAND terms should be the bare minimum for standards that the Commission requires by rule. Such a requirement would ensure that all competitive entrants have equivalent access to the intellectual property necessary to implement the standards required by rule. However, it is *not* enough to rely on the intellectual property policies of standards organizations and associations. Such groups generally require adherence to their intellectual property policies by their members, often as a condition of membership.²² However, there can be no guarantee that all intellectual property necessary for implementation of a standard is controlled by members of the developing organization.

²¹ *Notice* at ¶ 32.

²² *See, e.g.*, JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL: INTELLECTUAL PROPERTY AND INTEROPERABILITY IN THE GLOBAL SOFTWARE INDUSTRY 336-7 (1995).

Moreover, as with many areas of technology, intellectual properties of certain aspects of the proposed solution may be controlled by non-practicing entities.

The Commission should adopt by rule or reference only standards and technologies that are demonstrably licensed under RAND terms, so as to assure the public interest by enabling effective competition.

Additionally, the Commission should be aware that standardizing conditional access alone is not sufficient for interoperability: a secret key, certificate, or other cryptographic construct is also required. These are often protected as trade secrets.

IV. DOWNLOADABLE SECURITY ISSUES ARE ORTHOGONAL TO THE ALLVID DISCUSSION

In seeking alternative proposals, the Commission seeks comment on how the AllVid proposal would affect downloadable security.²³ Recently, in the context of the Fourth Further Notice, Commissioner McDowell wondered “[W]hatever happened to downloadable security?”²⁴ Nagravisision has commented on this aspect of the *Fourth Further Notice* in our Reply Comments.²⁵

Downloadable security is a misnomer. All widely-discussed forms of “downloadable security” do, in fact, require specific hardware components to be included in the receivers.²⁶ This specific hardware is not general purpose – it is neither a general-purpose chip (like a CPU) nor a

²³ *Notice* at ¶ 42.

²⁴ *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Fourth Further Notice of Proposed Rulemaking, CS Docket No. 97-80, PP Docket No. 00-67 (“*Fourth Further Notice*”) at ¶ 26.

²⁵ *Reply Comments of Nagravisision*, CS Docket No. 97-80, PP Docket No. 00-67 (June 28, 2010).

²⁶ The Beyond Broadband Technology solution requires a specific “secure microchip”, *Comments of Beyond Broadband Tech. LLC*, CS Docket No. 97-80, PP Docket No. 00-67 (filed June 14, 2010) (“*BBT Comments*”) at 10, sold for \$5.00 each, *id.* at 5, available only under license, *id.* at n.20. The now-abandoned Polycipher “DCAS” system also required a specific (and different) chip in a receiver, Brian Santo, *Night (Polycipher) Shift*, CEDMagazine.com (June 1, 2008).

general-purpose security chip (like a standard secure microcontroller). The Beyond Broadband Technology solution requires a specific security chip, which is sold under license for \$5 each.²⁷ The abandoned Polycipher “DCAS” system would have similarly required a different specific chip, sold with restrictions for a nontrivial sum.²⁸

In our Reply Comments to the Fourth Further Notice,²⁹ we ask the Commission to determine what the threshold (if any) is for the level of hardware that determines whether a conditional access system is “hardware-oriented” in the meaning of the Second Report and Order.³⁰

In any case, we believe that downloadable conditional access issues are orthogonal to the AllVid discussion. An AllVid adaptor may or may not be required to have separable security, and a certain amount of hardware is or is not allowed for “downloadable” conditional access systems. The two issues should be resolved separately.

V. USER INTERFACES SHOULD BE UNENCUMBERED

A successful competitive retail environment requires that retail devices have the capability to compete with both other retail devices and MVPD-provided devices. Historically, the cable industry has exercised significant control over the features and functionality of retail navigation devices.³¹ The Commission is attempting to address the hardware and certification aspects of these issues,³² and has had various complaints and proposals before it in the past.³³

²⁷ BBT Comments at 5.

²⁸ See Letter from James L. Casserly, counsel to Comcast Corporation to Marlene H. Dortch, Secretary, Fed. Communications Comm’n, CS Docket 97-80 (July 18, 2005); see also Jeff Baumgartner, *Onward, DCAS*, CedMagazine.com (Feb. 1, 2006), available at <http://www.cedmagazine.com/onward-dcas.aspx>.

²⁹ *Supra* note 25 at 5-6.

³⁰ See *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices*, Second Report and Order, 20 FCC Rcd. 6794, 70 FR 36040 (2005) at ¶ 35.

³¹ See *supra* note 13.

³² See Fourth Further Notice at ¶ 18.

Branding in consumer products is always important, and all the more so when addressing global markets and services. The look, feel, and functionality of user interfaces are integral to the consumer's satisfaction with the product. While form follows function, form can also constrain function. Restrictions on the user interface would stifle development at exactly the point in the product chain where innovative new capabilities are presented and offered to the consumer.

We believe that smart video devices must not be constrained in the way they compete for a competitive environment to develop. Smart video devices must be able to implement electronic program guides without restriction – including the freedom to integrate non-MVPD content with linear and interactive MVPD content. Simply put, there should be no restriction on disaggregation.

(continued) _____

³³ See Letter from Brian Markwalter, Vice President, Tech. & Standards, Consumer Electronics Ass'n, *et. al* to Marlene H. Dortch, Secretary, Fed. Communications Comm'n, CS Docket No. 97-80 (Nov. 7, 2006); Consumer Electronics Ass'n Comments on Third Further Notice of Proposed Rulemaking, CS Docket No. 97-80, PP Docket No. 00-67 (Aug. 24, 2007); Joint Comments of the Home Networking Proponents on Third Further Notice of Proposed Rulemaking, CS Docket No. 97-80, PP Docket No. 00-67 (Aug. 24, 2007).

CONCLUSION

Nagravision urges the Commission to:

- i) Resolve key structural problems that persist to the detriment of any attempt to implement Section 629, specifically by requiring Simulcrypt interfaces to enable competition among conditional access vendors, require supplier diversity to break the lock between conditional access and set-top box vendors, and establish third-party certificate issuance and certification;
- ii) Avoid selecting only partial solutions, like DTCP-IP, for the diverse needs of an AllVid network and thereby unintentionally inhibiting innovation;
- iii) Proactively ensure that necessary technology is available under RAND terms;
- iv) Separate the issues of downloadable security from the AllVid discussion; and
- v) Enable innovation through unencumbered user interfaces.

Respectfully submitted,

/s/

Robin Wilson
Vice President, Business Development
Nagravision
841 Apollo St.
El Segundo, CA 90245
robin.wilson@nagra.com

July 13, 2010