

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

In the Matter of:

Implementation of Section 304 of the
Telecommunications Act of 1996

CS Docket No. 97-80

Commercial Availability of Navigation
Devices

PP Docket No. 00-67

Compatibility Between Cable Systems and
Consumer Electronics Equipment

**COMMENTS OF
THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

William A. Check, Ph.D.
Vice President, Science & Technology

Daniel L. Brenner
Neal M. Goldberg
Loretta P. Polk

Andy Scott
Senior Director, Engineering

National Cable & Telecommunications
Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903

Paul Glist
Cole, Raywid, & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
202-828-9820
pglist@crblaw.com

February 13, 2004

SUMMARY

The Commission's Second Further Notice of Proposed Rulemaking poses questions concerning further implementation of the "Plug and Play" rules for digital televisions and other Unidirectional Digital Cable Products ("UDCPs").

First, the Commission sought comment on whether it should impose limits on the use of image constraint for non-broadcast programming. We oppose such limits. The Commission has already recognized that constraining the image of high value digital content that could be output over unprotected analog component interfaces was a necessary tool for making such high value content available to MVPDs. As long as the possibility exists for analog component interfaces to output HDTV ("HD") content without constraint, MVPDs are handicapped in negotiating with programmers concerned over unauthorized redistribution of high value programming. The cable and CE industries have agreed upon the technology for implementing image constraint, independent of copy control state.

Even if the agreed image constraint technology is invoked, UDCP manufacturers are permitted to use line doubling or other techniques to improve the perceived quality of an image constrained picture. New receivers that include component analog outputs are likely to also include digital ports, towards which viewers should be steered to advance the digital transition. The marketplace dynamics between cable operators and program suppliers will be the best forum for optimizing the use (or non-use) of constrained image triggers. Of course, if issues arise in the marketplace, the Commission remains able to address such issues as necessary and within its authority. Therefore, the Commission should permit image constraint for non-broadcast programming.

Second, the Commission sought comment on whether it should require pre-sale information disclosures to consumers in addition to the post-sale information required by the MOU and Commission rule. The limited scope of the MOU did not reflect any hostility to pre-sale information, but rather an understanding of potential limits on the Commission's authority that predated *Consumer Electronics Ass'n v. FCC*, 347 F.3d 291 (D.C. Cir. 2003). Cable operators consider it important that consumers have a full understanding of UDCPs in order to minimize the potential for confusion. Consumers should understand as they make purchase decisions that unidirectional "digital cable ready" devices do not have the necessary interactive functionality to, for example, order video-on-demand movies.

Third, the Commission asked if digital transmission and headend equipment requirements should apply to cable systems with channel capacity of less than 750 MHz. Given that 750 MHz and larger systems reach more than 80% of the total U.S. television households and that the economics of the smaller systems would be strained if subjected to these requirements, NCTA submits that the requirements should continue to apply only to systems with channel capacity of 750 MHz and greater.

Finally, the Commission sought comment on whether CableLabs should retain its status as an initial entity approving and/or rejecting new content protection technologies and outputs as well as comment on the appropriate standards for revoking approval for technologies and outputs that have been compromised. Output and security review of UDCP connectors is part of a transition from highly secure proprietary conditional access used internally by cable operators and in digital set-tops provided to cable subscribers, to retail DTVs with set-top functionality built inside. If new outputs or new security techniques do not provide sufficient security assurances, a new "digital hole" will be opened. That hole will undo conditional access, copy

control, image constraint, and the very tools that enable cable operators to negotiate with program suppliers for high value digital content to provide to their cable subscribers, while offering such program suppliers a reasonable assurance that such content will be protected from illegal access. In short, the proper operation of new outputs or new security techniques is vital to cable operators' core business.

CableLabs is the natural authority for that review. It is a world-respected laboratory staffed by trained professionals. CableLabs has demonstrated its ability to fairly and expeditiously draft specifications that are widely adopted (even world wide), and to test and certify multiple types of equipment. For example, over 370 retail DOCSIS-certified cable modems from over 65 vendors have been certified. Input from other industries is encouraged through the open Engineering Change Request process. The OpenCable project alone has over 500 companies participating.

CableLabs is a respected enabler of innovation—not an impediment. CableLabs was an industry leader in supporting the use of copy-protected digital connectors. It voluntarily developed the OpenCable Applications Platform (“OCAP”) specification ahead of schedule to support the nationwide portability of applications, such as program guides, on retail navigation devices. It developed the OpenCable specifications to promote market entry by competitive CE manufacturers well before any FCC “retail availability” requirements were adopted. It developed the necessary specifications to implement the CEA and NCTA voluntary agreements of February 22, 2000. It met every FCC-mandated milestone.

CableLabs' and the cable industry fully support retail availability. Cable operators want and need a retail presence to compete against DBS; and want innovation in retail products that will encourage customers to subscribe to cable services. CableLabs evaluates all proposals in a

reasonable, objective, and non-discriminatory manner. CableLabs has been engaged in constructive discussions with IT interests in order to develop digital rights management technology.

While CableLabs should be trusted with the task of approving new digital connectors and security technologies for devices that connect to, and have a potential to harm, the cable network and cable services, it is important to recognize that CableLabs is not the “sole initial arbiter” of approved technologies. The applicable agreements specifically create a parallel, independent path for program suppliers to approve new content protection technologies which will then be “deemed approved” by CableLabs. The Commission should permit CableLabs, and the program suppliers, to continue in their respective roles, as defined in the agreement between the cable and CE industries.

Efforts to harmonize the UDCP output review process with the similar process for broadcast flag outputs and technologies must recognize that the two processes arise from very different contexts. UDCP connectors can open a digital hole undoing conditional access and defeating the core business of the cable industry. By contrast, the programming to which the broadcast flag may be applied is available in unencrypted, free, over-the-air form for reception and copying by millions of embedded legacy devices. The Commission (rightly) rejected an expert level of robustness for the broadcast flag as “incongruous with the scope of protection offered by an ATSC flag system.” Likewise, while an output or security technology approved for UDCPs should be suitable for broadcast flag use, the reverse is not appropriate. We also suggest that new outputs or security technologies may be adopted for broadcast flag purposes by two paths. In the first path, objective criteria (similar to those used by CableLabs for UDCPs) would be applied by appropriate representatives of program suppliers to the broadcast industry,

subject to de novo review at the FCC. In the second path, any applicant could seek direct approval by the FCC.

TABLE OF CONTENTS

	<u>Page</u>
I. Constraining the Image of Non-Broadcast Programming	- 2 -
II. Consumer Information Disclosures	- 5 -
III. Applying Digital Transmission Standards to Smaller Systems	- 6 -
IV. Role of CableLabs in Output and Security Review	- 7 -
A. CableLabs Has a Track Record of Enabling Innovation in Constructive Collaboration with Manufacturers	- 8 -
B. Proper Functioning of New Outputs and New Security Technologies is Critical to the Protection of Conditional Access and to Cable Operators' Entire Core Business	- 11 -
C. CableLabs Is Only One Path for Approval of New Outputs and Security Technologies; the FCC and Program Suppliers Provide Another Path	- 14 -
D. CableLabs' Output and Security Review Criteria Are Fair and Objective	- 15 -
E. Revocation Processes Should Be Evaluated as Part of Output and Security Review	- 18 -
F. How to Harmonize Broadcast Flag and "Plug and Play" Output Reviews	- 19 -
CONCLUSION	- 21 -

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

In the Matter of:

Implementation of Section 304 of the
Telecommunications Act of 1996

CS Docket No. 97-80

Commercial Availability of Navigation
Devices

PP Docket No. 00-67

Compatibility Between Cable Systems and
Consumer Electronics Equipment

**COMMENTS OF
THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association (“NCTA”) hereby submits its comments in response to the Second Further Notice of Proposed Rulemaking (“*2dFNPRM*”) in this proceeding.¹

NCTA is the principal trade association of the cable television industry, representing operators serving more than 90 percent of the nation’s cable customers. These companies also provide high-speed access to the Internet and other services. NCTA’s members also include more than 200 cable program networks as well as companies that provide equipment and services to the cable industry. Cable operators also provide support for Cable Television Laboratories, Inc. (“CableLabs”), a nonprofit research and development consortium that has developed new specification-setting projects such as OpenCable, PacketCable, Cable Home and

¹ The Second Report and Order and Second Further Notice of Proposed Rulemaking were released on October 9, 2003. FCC 03-225, 2003 WL 22309173. The Media Bureau extended the comment date for the Second Further Notice to February 13, 2004 and the Reply Comment date to March 15, 2004. *Order*, DA 03-4085 (Dec. 23, 2003)

CableModem/DOCSIS² that have allowed for the widespread deployment of retail digital set-top boxes, cable modems, and other interoperable equipment bringing new digital broadband and video services to the American consumer.

I. Constraining the Image of Non-Broadcast Programming

In the *Second Report & Order* the Commission recognized that constraining the image of high value digital content that could be output over high definition component analog interfaces was a necessary tool for making such high value content available to MVPDs and protecting against the unauthorized copying and distribution of digital content. *SR&O* ¶¶ 62-64. Based on the recommendation of the cable and consumer electronics industries, the Commission only prohibited the use of image constraints with respect to unencrypted broadcast programming.³ However, the two industries made no recommendation on the use of image constraints for non-broadcast programming. The Commission allowed the use of image constraints for non-broadcast programming subject to notice, but asked if it should consider imposing limits on its use for non-broadcast programming. *SR&O* ¶64; *2dFNPRM* ¶ 82. The use of image constraints for non-broadcast programming is essential. The Commission should not prohibit their use and should instead allow market forces to determine when and how image constraints may be used.

Many of the technical standards agreed upon by the cable and CE industries and now included in the FCC's rules focus on the tools for securing outputs and for recognizing and respecting copy control signaling associated with high value digital programming delivered from cable systems to retail DTVs and similar UDCPs. However, not all outputs are protected.

² CableLabs®, DOCSIS®, PacketCable™, OpenCable™, OCAP™, CableCARD™, CableHome™ and Go2BroadbandSM are trademarks and servicemarks of Cable Television Laboratories, Inc.

³ The Commission, *sua sponte*, reconsidered the definition of "Unencrypted Broadcast Television" to eliminate a perceived competitive disparity for certain MVPDs. *Order on Reconsideration*, FCC 03-329 (rel. Dec. 23, 2003). The original definition caused no disparity and the revised definition will impact dual-use content in a way that will frustrate the application of encoding rules. NCTA will seek reconsideration of that revised definition separately.

Authorized digital outputs are protected by HDCP or DTCP.⁴ Standard definition analog ports are protected by Macrovision.⁵ But there is no standardized protection for high definition output over component analog ports. This means that programming which is supposed to be protected against copying can “leak” out of unprotected HD component analog ports without any copy controls whatsoever. An HD program marked for copy protection could be copied in its high resolution format and, with equipment now becoming more readily available, then be redigitized and subjected to precisely the kind of unauthorized copying and redistribution that is supposed to be prohibited by copy controls at the outset. This process for potential leaking of unprotected digital content is colloquially known as the “analog hole.”

In the *SR&O*, the Commission concluded that including the capability for constraining the image of non-broadcast programming was one effective tool in addressing the analog hole. It authorized the use of image constraints for non-broadcast programming subject to 30-day advance notice to the Commission. *SR&O* ¶ 64. The Commission has now asked for comment on whether Commission action is needed to govern the use of image constraints for non-broadcast programming. *2dFNPRM* ¶ 82.

Since the *SR&O*, the cable and CE industries have agreed upon the technology for implementing image constraint. One bit of the copy control information (CCI) byte is now dedicated to a Constrained Image Trigger (CIT).⁶ If the CIT signals image constraint, the UDCP device must reduce the picture resolution which exits from a high definition analog output of a UDCP to the visual equivalent of not more than 520,000 pixels per frame (*e.g.*, an image with

⁴ Exhibit B, § 2.2.1 to the DFAST License posted at www.cablelabs.com/udcp

⁵ Exhibit B, § 2.4 to the DFAST License posted at www.cablelabs.com/udcp.

⁶ The details are included in Exhibit A1, § 6.1.3 (“CIT- Constrained Image Trigger) to the DFAST License posted at www.cablelabs.com/udcp. The CE and cable industries also plan to submit this image constraint technology to SCTE as a modification to SCTE-41.

resolution of 540 vertical by 960 horizontal pixels for a 16:9 aspect ratio). The UDCP Manufacturer is permitted to enhance the Constrained Image using video processing techniques such as line doubling to improve the perceived quality of the image.

The CIT was structured so that it may be implemented independent of the copy control state for the program. That is, use of CITs with high definition digital programming is subject to bargaining in the negotiation of affiliation agreements between cable operators and program suppliers, separate from any contractual copy control settings. A program supplier could determine that a particular program should be marked for copy protection but need not be reduced in resolution over high definition component analog ports—essentially taking on the risk of unauthorized redistribution of redigitized high resolution programming in exchange for displaying full resolution programming through analog component outputs. Another program supplier might determine that it was unwilling to take that risk for its programming, and require image constraint triggers as a condition to supplying that programming to cable operators whose customers may have UDCPs with unprotected analog component outputs. The marketplace decides.

Cable operators need the flexibility to negotiate both types of agreements with programmers in order to maximize the programming available to cable subscribers. In all cases, broadcast content will not be subject to image constraint, as is consistent with consumer expectations and FCC rules. Even for non-broadcast programming that under negotiated terms would be subject to the CITs, UDCP Manufacturers can nonetheless use line doubling or other techniques to improve the perceived quality of the image. The only report with which we are

familiar indicates that there is no noticeable difference in viewing quality between constrained and unconstrained images when viewed over legacy high-definition television receivers.⁷

The digital transition will be further advanced by permitting the use of image constraint for non-broadcast programming. New receivers that include component analog outputs are likely to also include protected digital ports. Public awareness that uncompressed, full resolution images are available from protected digital ports (*e.g.*, DVI/HDCP or HDMI/HDCP) should help migrate customers away from analog component interfaces to copy-protected digital feeds.

Image constraints have not yet been implemented in the field. NCTA submits that it would be premature for the Commission to attempt to define the operation of the market at this stage. We are confident that the marketplace dynamics between cable operators and program suppliers will be the best forum for optimizing the use (or non-use) of CITs. We are also confident that if there is significant consumer dissatisfaction arising from that marketplace, the Commission will learn of it and be able to address any issues that it believes to be necessary and within its authority. For this reason, the Commission should permit the use of image constraint for non-broadcast programming.

II. Consumer Information Disclosures

The Commission has asked whether consumers should be provided with additional pre-sale information about the capabilities of UDCPs and their need for CableCARDS. *2dFNPRM*

¶ 81. The cable operator-CE manufacturer December 2002 Memorandum of Understanding (“MOU”) included requirements for only post-sale consumer information, but that did not

⁷ Letter of Bruce Boyden to Marlene H. Dortch in CS Docket No. 97-80, May 7, 2003 (reporting ex parte presentation by MPAA that “legacy HDTV displays do not currently fully resolve 1080 by 1920 television content. As a result, when a 1080i image is constrained to 960 by 540 resolution and then up-converted for display on a legacy HDTV display, there is no noticeable difference between the resulting image and an unconstrained image sent to the same display.”)

reflect any aversion to the provision of pre-sale information to consumers. Rather, it reflected the parties' understanding of potential limits on the Commission's authority over retailers and, prior to *Consumer Electronics Ass'n v. FCC*, 347 F.3d 291 (D.C. Cir. 2003), the parties' understanding of jurisdictional limits under the Communications Act over equipment manufacturers.

Cable operators consider it important that consumers have a full understanding of UDCPs in order to minimize the potential for confusion. Consumers should understand as they make purchase decisions that unidirectional "digital cable ready" devices do not have the necessary interactive functionality to, for example, order video-on-demand movies. NCTA has worked with cable operator representatives and CableLabs to complete a set of frequently asked questions that may be used by cable operator customer support representatives to inform cable customers of the capabilities of UDCPs, and provide consistent answers to anticipated queries consumers may have when calling their local cable operator help-desk for support. Additionally, the cable industry has partnered with the CE industry to develop a common logo that will facilitate consumer awareness of "Digital Cable Ready" ("DCR") and "Interactive Digital Cable Ready" ("iDCR") devices.⁸

III. Applying Digital Transmission Standards to Smaller Systems

The cable and CE industries agreed that certain digital transmission and headend requirements would only apply to systems that had been upgraded to an activated channel capacity of 750 MHz and greater. *SR&O* ¶ 17. In the earlier comment phase, no comments were received objecting to this requirement. In the Second Further Notice, however, the Commission

⁸ See Letter from Neal M. Goldberg, NCTA to Marlene H. Dortch, Secretary, dated January 21, 2004 ("NCTA Status Report"). See also Letter from Michael D. Petricone, CEA, to Marlene H. Dortch, Secretary, dated January 21, 2004 ("CEA Status Report") (confirming that the parties finalized "DCR" and "iDCR" logos)

has asked whether these headend and transmission standards should be applied to systems with an activated channel capacity of 550 – 750 MHz as well. *2dFNPRM* ¶ 80. For the reasons stated below, the Commission should not extend these requirements to these systems.

The parties had agreed upon the 750 MHz cut off for two reasons. First, such systems could meet the headend specification with manageable additional investments, while 550 MHz systems could not. Second, the national footprint of 750 MHz systems was sufficient to sustain a national market in retail equipment. More than 90 million homes (more than 80% of the total U.S. Television Households) are passed by cable plant with a capacity of 750 MHz or higher.⁹

The MOU went on to provide that UDCPs “may not impose additional investment requirements on the cable distribution network, beyond MSO obligations specified in this MOU.”¹⁰ The amount of effort and resources being invested by the cable industry to implement the MOU and the current rules, to negotiate the next bi-directional phase, and to make the digital transition work is overwhelming. We respectfully request that the Commission continue to apply its “plug and play” headend and transmission rules only to systems with an activated channel capacity of 750 MHz or greater.

IV. Role of CableLabs in Output and Security Review

The Commission has asked a series of questions about the role of CableLabs in the review of outputs and associated content protection technologies, the potential for digital rights management, wireless and encryption-based technologies to be utilized, the objective criteria to be used, and whether the Commission or a third party should assume the role currently assigned to CableLabs. *2dFNPRM* ¶¶ 83-85. The Commission has also asked a series of related

⁹ NCTA 2003 Year-End Industry Overview, at 2, 20 (available online at http://www.ncta.com/pdf_files/Overview.pdf).

¹⁰ MOU ¶ 3.12, available at *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Further Notice of Proposed Rulemaking, 18 FCC Rcd 518, 547 (1997) (“*FNPRM*”).

questions concerning the standards and process for revocation of previously approved connectors and content protection technologies that have been compromised or become insecure. *Id.* ¶ 86.

A. CableLabs Has a Track Record of Enabling Innovation in Constructive Collaboration with Manufacturers

We begin by addressing the Commission's stated concern that "CableLabs is not a standards-setting body;" that it has a "proposed role as the sole initial arbiter of outputs and associated content protection technologies to be used in unidirectional digital cable products;" and that it might retard "innovation." *2dFNPRM* ¶ 83. CableLabs is a research and development consortium of cable television system operators serving North America, South America, and Europe. It is a world-respected laboratory staffed by trained professionals.¹¹ CableLabs has an enviable track record of working collaboratively and successfully with manufacturers in the DOCSIS, OpenCable, and Packet Cable programs.¹² Through its Go2Broadband service,

¹¹ CableLabs was founded in 1988 as a non-profit research and development consortium. There are approximately 130 employees and consultants at CableLabs. Its chief executive officer is a research scientist who has worked at PBS, CBS, and ABC; who helped organize and establish the Advanced Television Systems Committee; who chaired the committee that eventually developed CCIR (now ITU-R) Recommendation 601, a world-wide television standard for digital signals; and who currently serves as chairman of Study Group G9, an ITU-T committee charged with the responsibility of recommending worldwide standards for cable television. The qualifications of other senior staff are set out at <http://www.cablelabs.com/about/seniorstaff>. CableLabs has no affiliation with manufacturers and its focus has been on certifying equipment that will satisfy interoperability requirements and enhance the provision of cable services.

¹² "Samsung Electronics Receives CableLabs® Certified™ Status for Integrated Digital Television;" "Panasonic Introduces First Cable-Ready HDTV At CEDIA; Set With CableLabs Certification Leads The Way For HDTV Penetration," available at http://www.cablelabs.com/news/pr/2003/03_pr_oc_samsung_cert_121703.html; http://www.panasonic.com/consumer_electronics/pressroom/cont2.asp?Filter=12&cont_id=515. CableHome™ is a CableLabs-managed initiative that, coupled with cable broadband service, allows for the distribution of broadband service throughout a consumer's home. The initiative offers the consumer a secure and managed residential gateway that can be connected to the cable network in a plug-and-play fashion, offloading much of the technical burden inherent in home networking from the consumer to cable operator. There are also now more than 20 devices certified or qualified in four PacketCable certification events. Altogether, devices from more than 80 manufacturers have been certified by CableLabs under the various initiatives, including products from Panasonic, Samsung, Motorola, Scientific-Atlanta, Thompson, Toshiba, Texas Instruments, Linksys, Pioneer, D-Link, Ericsson, General Instrument, and Sony. For the complete listing, see: <http://www.cablelabs.com/certqual/whocertified.html>. See *Commercial Availability of Navigation Devices*, Order on Reconsideration, 14 FCC Rcd 7596 para. 41 (1999) (Several milestones in OpenCable process occurred allowing entities outside the cable industry to make input into interface design specifications and "no party has brought forth evidence that their input is not being accepted or considered").

CableLabs also provides retailers and consumers with information about the services provided by cable operators that are available at a given consumer address.

There are now over 400 DOCSIS and CableHome devices that have received certification or qualification status in the last four years of CableLabs testing. CableLabs has also developed and implemented other interoperable technology platforms such as PacketCable and CableHome and started the entire process for retail set-top boxes and UDCPs with its OpenCable initiative. PacketCable is a CableLabs-led initiative to define a common platform to deliver advanced real-time communication services, such as VoIP, over two-way cable plant. Panasonic and Samsung have already been certified for several models of integrated DTVs that connect directly to cable television systems and receive digital services without requiring a set-top box.

While it is not an ANSI standards body, CableLabs' processes are no less fair and objective. CableLabs specifications are drafted with input from the relevant manufacturing sector. The reason is obvious—drafting specifications that do not work for manufacturers, or that will not be implemented, is a wasted effort. Active specification working groups include interested parties from the CE, IT, content, and cable communities. Once a specification is issued, any company, from any industry, may submit an Engineering Change Request (“ECR”) that is fairly and objectively reviewed by an ECR Working Group that draws members from the interested industries. Many of the specifications CableLabs has developed under its processes have been submitted to, and approved as standards by, the Society of Cable and Telecommunications Engineers (“SCTE”)—an ANSI-accredited standards development organization—or other standards bodies, including the International Telecommunications Union (ITU) for world-wide standards (e.g., DOCSIS, OCAP, CableHome, and PacketCable).

CableLabs has also demonstrated its ability to fairly and expeditiously test and certify multiple types of equipment. To date, over 370 retail cable modems from over 65 vendors have been certified.

As shown by the initiation of the OpenCable project prior to the adoption of any FCC rules in that area, CableLabs and the cable industry fully support retail availability. Operators want and need a retail presence to compete against DBS providers that have flooded retail outlets with their own proprietary equipment. Cable operators are *service* providers, who want innovation in equipment that delivers those services so consumers will be encouraged to subscribe to cable services.

The cable industry's commitment to the success of retail availability is a matter of record. It is worth reiterating how essential CableLabs has been in fulfilling that commitment.

- The cable industry, *through CableLabs research*, was a leader in supporting the use of copy-protected digital connectors (both the 1394/DTCP digital interface and the DVI/HDCP connector) to induce content providers to supply high quality programming to cable operators.
- The cable industry *through CableLabs* met every FCC-mandated milestone for developing specifications to enable the manufacture of navigation devices that could be sold at retail and which would work with operator-supplied POD modules – modules which were available by the FCC's July 1, 2000 deadline. As early as the January 2001 Consumer Electronics Show, Panasonic demonstrated that the POD module worked on digital TVs with integrated set-top box functionality.
- CableLabs' OpenCable effort was initiated and funded by the cable industry well before any FCC "retail availability" requirements were adopted.
- *CableLabs developed the necessary specifications* to implement the CEA and NCTA voluntary agreements of February 22, 2000 to allow "integrated" DTV sets to be connected directly to digital cable systems.
- The cable industry, *through CableLabs*, voluntarily developed the OpenCable Applications Platform ("OCAP") specification ahead of schedule. In addition to enhancing the portability of set-top boxes and DTV sets, OCAP supports the nationwide portability of applications, such as program guides, on such devices.
- OCAP was specifically agreed upon in the MOU as the vehicle for delivering electronic program guides to bi-directional devices with national portability. It has

also been adopted in total by Korea. It is in the process of standardization at SCTE (SCTE-90), ATSC and the International Telecommunications Union (ITU).

In short, CableLabs has proven to be a respected enabler of innovation—not an impediment. Its role in output and security review is critical to the success of retail availability, to bringing high value content to cable subscribers, and to the overall digital transition. As NCTA explained in its December 29, 2003 Petition for Reconsideration, the MOU was delicately structured to protect conditional access; to preserve the economic structure for the delivery of cable services; and to assure that cable has the technological tools to provide even more attractive services to customers

B. Proper Functioning of New Outputs and New Security Technologies is Critical to the Protection of Conditional Access and to Cable Operators' Entire Core Business

Congress and the Commission have recognized the importance of protecting cable's signal security as well as preventing harm to the cable network in the course of adopting rules to facilitate the commercial availability of navigation devices.¹³ Section 629 of the Communications Act made signal security prominent and prohibited the Commission from adopting regulations that would jeopardize security of programming and services.¹⁴ CableLabs plays a vital role in the effort to protect signal security and prevent harm to the cable network.

Today, cable operators deliver secured programming from cable headends to cable customers by using conditional access technology at the headend linked to companion technology in the set-top boxes. The technology is proprietary to Scientific-Atlanta, Motorola,

¹³ Petition for Reconsideration or Clarification of the National Cable Telecommunications Association, dated December 29, 2003 at 5-14.

¹⁴ 47 U.S.C. 549(b); H.R. Conf. Rep. No. 458, 104th Cong., 2nd Sess., at 181 (1996); H.R. Rep. No. 204, 104th Cong., 2nd Sess., at 112.

and NDS. Utilizing this conditional access technology allows cable operators to deploy set-top boxes to their subscribers and authorize or deauthorize services. It allows customers to buy discrete premium channels, to order pay-per-view events and video-on-demand, to subscribe to expanded tiers, to buy only the basic tier, or to buy basic plus premium services without having to "buy-through" the tier. Conditional access technology permits a customer to make changes in his or her service offerings without waiting at home for an installer, and without a cable operator needing to dispatch a truck, by delivering secure codes to the set-top boxes activating or deactivating specific program services. With the addition of copy control and image constraint signaling, these devices provide the tools needed by cable operators so that they can confidently negotiate with program suppliers for the high value programming desired by cable customers. Without the secure handling of such authorization codes and associated copy protection controls, the operator cannot offer the services that have come to be enjoyed by his customers, cannot be assured of payment, cannot have adequate protection against theft, and cannot assure program suppliers that the programming is being used only as contracted for in their affiliation agreements.

Now that set-top boxes and other "Host" devices can be manufactured by any vendor, it is essential to preserve the security that has to date been insured by the contractual relationship between cable operators and their traditional set-top box suppliers. The new POD-Host interface provides the same high value programming to consumer-owned devices that need to be trusted to obey the access and copy control rules associated with the programming. It provides full access to the content: at the POD-Host interface, the programming received from the headend is decrypted, re-encrypted with the DFAST protection, and passed to the UDCP (along with the copy control bits) for display, possible recording or storage. The UDCP must be trusted to obey

the copy control rules associated with the programming and to not change or delete the codes. The UDCP must assure that “copy once” programming is only copied one generation. The UDCP must assure that there are no insecure outputs, or insecure points for hackers to attack, that would defeat these security and copy protection rules.

These security rules are protected by algorithms, security certificates, and key exchanges. If compromised due to the weaknesses of a trusted UDCP, these security measures could be detected, copied or used and cloned for pirate products. If new outputs or new security techniques do not honor these protections, a new “digital hole” will be opened that will undo conditional access, copy control, image constraint, and the very tools essential for cable operators to conduct their core business.

Protecting each point of hardware and software vulnerability in an output or security technology is the art of the security specialist, and it is not easy. As the Commission recognized, copy protection tools must work in order to assure access to programming. “Service theft is a serious matter. Failure of the access control or security systems will interfere with incentives to produce programming for the market and such a failure would increase the cost of service to those who do subscribe.”¹⁵ Programmers repeatedly and recently have made it clear to cable operators that they will place their most desirable product on platforms that have these security tools working if cable does not assure security.¹⁶ The importance of making this work cannot be

¹⁵ *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking, 12 FCC Rcd 5639, ¶ 31 (1997)

¹⁶ This point has been driven home in discussions in private industry settings, as well as in public filings. See, e.g., Comments of the Motion Picture Association of America, Inc., in CS Docket No. 97-80 (March 28, 2003) at 5 (“Content providers have long suggested to the cable industry that any license governing cable set-top boxes needs to include sophisticated content protection, so that cable is not placed at a competitive disadvantage in attracting quality programming vis-à-vis competing services such as satellite.”); Letter from Fritz E. Attaway, Senior Vice President of Government Relations, MPAA, to W. Kenneth Ferree, Chief, Media Bureau, Federal Communications Commission, June 5, 2002, at Attachment p. 1 (responding to “PHILA Hoedown” questions, to the same effect); Letter from Fritz E. Attaway to Magalie R. Salas, PP Docket No. 00-67; CS Docket No. 97-80 (September 6,

overstated: for manufacturers, building UDCPs is an incremental business; but for cable operators, getting it right at the outset is essential to cable operators' entire core business.

This is why Congress specifically instructed the FCC to assure that its rules did not compromise cable security. "Cable and other telecommunications operators have a valid interest, which the Commission should continue to protect, in system or signal security and in preventing theft of service and, therefore, the Commission may not prescribe regulations which would jeopardize signal security...."¹⁷ CE manufacturers have never before built integrated DTVs with digital cable set-top box functionality built inside, and they have never been responsible for protecting the copy control signals and business models that make the cable industry work. No one can be unconcerned about the consequences of error, whether intentional, negligent or accidental.

C. CableLabs Is Only One Path for Approval of New Outputs and Security Technologies; the FCC and Program Suppliers Provide Another Path

Given its track record, CableLabs was an obvious selection for output and security review.¹⁸ But CableLabs was not given that role exclusively. The cable industry believes that there should be at least one alternative path for having authorized outputs and security approved, and specifically provided for this in the MOU. The DFAST Technology License Agreement and FCC rules provide two paths for approval. One is through CableLabs, with a de novo review at the FCC if any party is dissatisfied with an approval or a disapproval of a new output or security

2000)("Either devices will respond to copy management instructions, or they won't. If they won't, they cannot receive high value, copy protected content."); Todd Shields, "Fast-Tracking Plug & Play," Mediaweek.com (April 7, 2003) ("Attaway said if cable alone adopts the plug-and-play standard, studios may shift movies to satellite services that could better defend against content theft.")

http://www.mediaweek.com/mediaweek/headlines/article_display.jsp?vnu_content_id=1858405

¹⁷ H.R. Conf. Rep. No. 458, 104th Cong., 2nd Sess., at 181 (1996).

¹⁸ There are also technical reasons for investing that trust in CableLabs. An approved output must be tested against an approved test suite. CableLabs has the equipment to perform such testing; and a detailed understanding of the Joint Test Suite that was jointly crafted with CEA. CableLabs and CEA are the parties responsible for updating the Joint Test Suite in order to accommodate new outputs.

technique. Thus, a disappointed output proponent could obtain review (and potentially approval) at the FCC. Similarly, a program supplier unhappy with a newly approved output could appeal a grant and could obtain review (and potentially disapproval) from the FCC. The second path is explicitly market based: the key program suppliers (on whom the cable industry is dependent for programming) may directly approve outputs and associated content protection technologies and have them added as approved outputs, which are then “deemed” approved by CableLabs.¹⁹ Thus, CableLabs is not “the sole initial arbiter of outputs and associated content protection technologies.”

D. CableLabs’ Output and Security Review Criteria Are Fair and Objective

The Commission has also asked what standards should be applied to such output and security review, posing as a point of comparison the “functional” criteria proposed by Microsoft Corporation and Hewlett Packard Corporation. Under the Compliance Rules of the DFAST Agreement, certain enumerated digital outputs and content protection technologies are allowed on UDCPs—1394/DTCP, DVI/HDCP, and HDMI/HDCP. Additionally, CableLabs may approve new digital outputs or content protection technologies.

CableLabs is in the process of finalizing the objective review criteria for this process.

The review criteria include:

- **Video Transport**

- Is the video transport method clearly defined?
- Are the methods defined for translating and delivering CCI from the CableCARD across the POD-Host Interface into the proposed device environment or profile?

¹⁹ DFAST License Agreement, Exhibit B (Compliance Rules) ¶ 2.4.4, *available at FNPRM*, 18 FCC Rcd at 593.

- **Security Interfaces**
 - How is the security used on the video transport and how is the transport associated with content protection profiles (or encoding rules) and the methods for authenticating and protecting the content protection profiles?
 - What are the key generation, key protection and key exchange methods used?
 - Are there obvious areas where content is in the clear?
- **Points of Attack and System Weaknesses**
 - Can technology be circumvented somewhere?
 - Where are the lowest barriers to be attacked?
 - Where will the hacker attack and what resources are required?
 - What are possible weaknesses/threats and what is the trade-off of security versus the applied costs?
- **Effectiveness of proposed technology**
 - Does the proposed technology adequately protect content?
- **Security Processing**
 - Are the keys and secrets protected from reading and writing during the cryptographic calculations?
 - Are CCI, image constraint, and other controls protected throughout the system design?
- **Revocation and Renewability of keys**
 - Does the product provide a system key revocation solution?
 - Does the product provide a system key renewability solution?
- **New Algorithms**
 - What is the relative strength of the algorithm?
 - What is the relative strength of authentication with respect to other technologies?

- **DFAST/JTS Consistency**

- Does the proposed output/technology interfere with a UDCP device’s meeting its DFAST or testing obligations?
- Does the proposed output/technology interfere with OpenCable devices and interfaces?
- Does the proposed output/technology raise interoperability issues with other UDCP devices and interfaces?

- **Licensing Terms**

- Does the license include the Robustness Rules, Compliance Rules, Conformance testing, Change provisions (to the technology or the license terms), IPR indemnity or other IPR arrangements (*e.g.*, a patent pool), Warranty Provisions, Term, and a list of known relevant patents?
- Are the terms of use reasonable and fair? Is the technology offered royalty-free, or does it include commitments to offer reasonable and non-discriminatory (“RAND”) license terms.
- What license fees are required annually and on each device?
- How do the Robustness rules fit with other licensing requirements?

- **Burden on Cable Network**

- Are the Revocation and Renewability solutions easily adapted by an MSO so it can use Selective Denial of Service? (For example, it would be difficult to propagate twenty different sets of SRM messages.²⁰)
- Are there operational burdens placed on MSOs and other content distributors? Under the MOU, UDCPs may not impose additional investment requirements on the cable distribution network, beyond MSO obligations specified in the MOU.

Once these criteria are finalized, CableLabs will evaluate all proposals in a reasonable, objective, and non-discriminatory manner. CableLabs will document the reasons for approval, or disapproval, of the submission. A decision will be made within 180 days of receipt of a complete submission.²¹

²⁰ System Renewability Messages (SRMs) are lists sent to devices indicating, for example, that certain identified security certificates associated with a specific content protection technology have been cloned or compromised.

²¹ DFAST License Agreement, Exhibit B (Compliance Rules) ¶ 2.4.4, *available at FNPRM*, 18 FCC Rcd at 593.

CableLabs has been engaged in constructive dialogue with information technology interests in order to develop digital rights management technology. As a result of these discussions, additional consumer choices could be opened up as, for example, they facilitate the entry of personal computers as robust, compliant UDCPs. The process criteria noted above may be refined as an outgrowth of this review. It should be clear that these criteria and this process will serve the Commission's interest in an objective review process that focuses on functional criteria.

E. Revocation Processes Should Be Evaluated as Part of Output and Security Review

The Commission has also asked how revocation may be handled. The answer to this will vary according to output and security technique. Some outputs may be so compromised that only a substantial response (such as turning off the insecure port through selectable output control) can address the compromise. Other techniques (for example, some versions of DRM) can revoke discrete certificates associated with cloned devices, and renew and restore those certificates when proper authorization has been purchased. There is no single rule that covers every technique.

For example, in DTCP, the 5C license provides that program suppliers may, after an agreed-upon process, send SRM messages through various media (*e.g.*, a DVD that will "play" through a 1394/5C port and update the file of revoked licenses). But in practice, these SRM messages have not yet been deployed by studios. For the security certificates embedded in UDCP Host devices, there is an elaborate procedure for addressing cloned and stolen certificates. Grandfathering such cloned devices, as suggested in the *2dFNPRM*, would not be appropriate, because it would defeat the security afforded by the certificate validation process. Cable operators can also utilize service denial or service limitations to address compromised devices—

a technique not available for other technologies such as non-compliant DVD players. As a consequence, NCTA recommends that the revocation process appropriate to each security technique be evaluated in connection with output and security approval.

F. How to Harmonize Broadcast Flag and “Plug and Play” Output Reviews

In both this proceeding and the “Broadcast Flag” proceeding,²² the Commission has sought comment on what is the appropriate means for reviewing authorized outputs and content protection technologies, and whether the output review for UDCPs can or should be harmonized in some manner with the output review for the broadcast flag. *R&OFNPRM* ¶¶ 61, 62, 64.

Questions concerning appropriate output review mechanisms for UDCPs arise in a different context than do similar questions regarding such mechanisms for devices that implement the broadcast flag. Therefore, while on their face it appears that the questions raise similar, if not identical issues, that does not mean identical output review mechanisms should be applied in both contexts. As described above, output and security review of UDCP connectors is part of a transition from highly secure proprietary conditional access used internally by cable operators and in digital set-tops provided to cable subscribers, to retail digital television sets and other UDCPs with set-top functionality built inside. If new outputs or new security techniques for such UDCPs do not provide sufficient security assurances, a new “digital hole” will be opened. That hole will undo conditional access, copy control, image constraint, and the very tools that enable cable operators to negotiate with program suppliers for high value digital content to provide to their customers, while offering such program suppliers a reasonable assurance that such content will be protected from illegal access. In short, the proper operation of new outputs or new security techniques is vital to cable operators’ core business.

²² See *In re Digital Broadcast Content Protection*, Report and Order and Further Notice of Proposed Rulemaking, 2003WL 22494589 (Nov. 4, 2003) (“*R&OFNPRM*”)

By contrast, the broadcast flag is a new adjunct to the broadcast business, and is being implemented in an environment in which the underlying “secure” product is by intent and design available unencrypted, free, over-the-air and available for reception and copying by millions of embedded insecure legacy devices. This environment is quite different from the UDCP environment in which programming is distributed on an encrypted secure network.

It is this different context that led the Commission to (rightly) reject an expert level of robustness for the broadcast flag as “incongruous with the scope of protection offered by an ATSC flag system.” *R&OFNPRM* ¶ 46. Likewise, there is a different level of review appropriate for outputs and security technologies of UDCPs and for outputs and security technologies for the broadcast flag.

NCTA has described above the dual review mechanisms available for adding outputs or security technologies for UDCPs. We submit that any output or security technology that is approved in that context and under those criteria should be automatically deemed approved for broadcast flag use. On the other hand, it is not necessarily the case that an output or security technology that meets the “ordinary user” level applied to the broadcast flag is automatically appropriate for the high-value, early release content secured by UDCP encryption and copy control technologies. Thus, to harmonize the two regimes, we suggest that an output or security technology that is approved and added to the Compliance Rules for UDCPs be automatically approved for broadcast flag purposes. An output or security technology that is approved for broadcast flag purposes should so note that approval in submitting for review under the UDCP Compliance Rules, but that does not in and of itself qualify it for inclusion under the Compliance Rules without further review. As a practical matter, it is worth noting that the UDCP Compliance Rules process provides a significant role to the principal sponsor of the broadcast

flag rules. The MPAA has expressed concerns that their member studios have no voice in this process. But, the MPAA member studios can themselves approve an output for UDCP use; and have the right to force any CableLabs determination to be reviewed by the FCC—practically assuring themselves a key voice under either path.

With respect to the process for adding outputs or security technologies for broadcast flag purposes, we believe that the structure adopted for UDCPs is a helpful example of how to structure the process used for approval of broadcast flag technologies. Prior Comments in the broadcast flag proceeding have revealed a reluctance to place sole control of the “Table A” process with MPAA’s member studios. On the other hand, there is a benefit to allowing private industry to adopt outputs and security technologies without requiring every innovation to obtain government approval. We suggest that two paths be provided for adding outputs or security technologies for broadcast flag purposes. In the first path, objective criteria (similar to those used by CableLabs for UDCPs) would be applied by appropriate representatives of program suppliers to the broadcast industry, subject to de novo review at the FCC. In the second path, any applicant could seek direct approval by the FCC, eliminating concerns that a single entity can block approval of a new output or security technology.

CONCLUSION

For the reasons stated above, the Commission should: (1) permit the use of image constraint for non-broadcast programming; (2) reiterate the importance of providing consumers with pre-sale information about the capabilities of UDCPs; (3) maintain its current “plug and play” headend and transmission rules which apply only to systems with an activated channel capacity of 750 MHz or greater; and (4) permit CableLabs to maintain the role agreed upon by the cable and CE industries in approving content protection outputs and technologies in

recognition of its central role in advancing innovation in general, and cable compatibility with CE products in particular.

Respectfully submitted,

/s/ Daniel L. Brenner

William A. Check, Ph.D.
Vice President, Science & Technology

Andy Scott
Senior Director, Engineering

Paul Glist
Cole, Raywid, & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
202-828-9820
pglist@crblaw.com

February 13, 2004

Daniel L. Brenner
Neal M. Goldberg
Loretta P. Polk

National Cable & Telecommunications
Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903