

**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

**REPLY 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

March 15, 2004

## SUMMARY

**Image Constraint.** The Comments confirm that allowing for image constraint does not reduce consumer options, but facilitates more choice, such as in making available early release movies that would not otherwise appear on cable without the tools for constraining HD images that are output over unprotected component analog ports. The empirical information submitted confirms that image constraint would have no noticeable effect on current consumers, because the constrained image displays cannot be distinguished from a HD image given the actual resolution of the legacy TVs at issue. With respect to new devices, if UDCP manufacturers include component analog ports with image constraint capability, they may use line doubling or other techniques to improve the perceived quality of an image constrained picture. But they may also include protected digital ports, which customers should be encouraged to use 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 image constraint. There is no basis for limiting its use for non-broadcast programming at this time.

**Consumer Education.** Consumers should have information as they make purchase decisions about unidirectional “digital cable ready” devices. NCTA believes that there should be multiple paths for communicating the capabilities and limitations of devices, including the cable industry’s educational efforts detailed in our initial Comments, the press, post-sale material, and pre-sale information provided by retailers. Retailers routinely describe functionalities such as 480p or 1080i resolutions, effective viewing angle, on-screen menus, component video, S-video, DVI and other connectors, internal HDTV tuner or not. Retailers should likewise be informing customers that unidirectional “digital cable ready” devices will need CableCARDS and do not have the necessary interactive functionality to, for example, order video-on-demand movies.

Retailers should inform the Commission of what they will tell customers about the capabilities and limitations of these UDCPs.

**550 MHz Systems.** There is consensus that the Commission should continue to apply its “plug and play” headend and transmission rules only to systems with an activated channel capacity of 750 MHz or greater.

**New Outputs and Content Protection Technologies.** CableLabs’ role as *one* avenue for approving new outputs and content protection technologies for UDCPs in this process is supported by the manufacturers seeking to build into this market. The principal content providers are also willing to trust CableLabs to maintain essential network security. DBS’s objection is misplaced: CableLabs’ approval is not required for new interfaces on *DirecTV*’s set-top boxes. Because the FCC exempts DBS from the requirement to use or accommodate the POD-Host interface, DirecTV may build or contract for any outputs DirecTV desires.

Most parties agree that the approval process for UDCPs and for broadcast flag should not be unified because they operate in different regimes (*e.g.*, one encrypted and secure, the other free, in-the-clear, over-the-air) with different functional requirements (*e.g.*, one with copy protection, the other without it). But approval under the more rigorous UDCP standard should also suffice for the broadcast flag.

Several parties have submitted proposals for the specific standards and procedures for approving UDCP outputs and content protection technologies. The variations in supposedly “objective” and “functional” words and phrases will actually skew the outcome towards specific and often proprietary outcomes. For example, Microsoft and Intel favor pure software solutions that can be implemented far more readily in PCs than in retail CE products. Some parties are seeking to insulate their patent portfolio from any FCC inquiry into their license terms. Others

note that without license review, selectable output, or both, a patented technology installed in UDCPs could expose third parties to unexpected, uncontrolled license fees. Most proposals overlook some crucial fundamentals—such as how “effective” does the technology have to be in protecting content; the ability of the technology to actually transport video from cable to the consumer or to deliver the cable services for which the UDCP is actually licensed; and whether the technology interferes with a device’s obligations under the rest of the rules and agreements. This Reply includes a detailed comparison of each proposal attached as Exhibit A.

The criteria proposed by NCTA and CableLabs strikes a sensible middle ground. They require evaluation of the security elements addressed by the other proposals, but adopt approaches that facilitate innovation with connectors. They do not “discriminate” for or against PCs. They pose the relevant questions, allow engineering and cost tradeoffs to be made, and are subject to review at the FCC. All parties can gain helpful experience under this regime without jeopardizing security. It would be a mistake to try to establish all the answers in advance in an FCC rule. It would also be a mistake to permit self-certification of outputs and content protection technologies, when it is now obvious that revocation will be subject to significant objections, delays, and even request for permanent grandfathering of compromised outputs. The Commission should permit CableLabs to maintain its agreed-upon role in approving outputs and content protection technologies.

## TABLE OF CONTENTS

	<b>Page</b>
SUMMARY .....	i
I. Constraining the Image of Non-Broadcast Programming .....	1
II. Consumer Information Disclosures .....	6
III. Applying Digital Transmission Standards to Smaller Systems .....	7
IV. Role of CableLabs in Output and Security Review .....	8
A. Why CableLabs is the Natural Candidate for Approving Outputs And Security Technologies.....	8
B. DBS Remains Free to Define, Buy and Build Security and Outputs Without CableLabs or Any Approval.....	9
C. Standards and Approaches.....	10
1. Security Interfaces .....	12
2. Effectiveness .....	13
3. License .....	14
4. Relationship of UDCP Approval to the Broadcast Flag .....	16
5. Video Transport.....	16
6. DFAST/JTS Consistency .....	17
7. Burden on the Cable Network.....	18
D. The CableLabs Approach .....	19
1. Security Interfaces/Security Processing/New Algorithms/Points of Attack.....	19
2. Effectiveness .....	19
3. Licensing Terms.....	20
4. Relationship to Broadcast Flag .....	21
5. Video Transport .....	21
6. DFAST/JTS Consistency .....	21
7. Burden on the Cable Network.....	21
E. Why CableLabs is Preferable to an Inter-industry Panel or Self-Certification.....	22
F. Revocation .....	25
V. Other Issues.....	27
CONCLUSION.....	28
EXHIBIT A	
NCTA/CableLabs Comparison of Output Review Proposals.....	1A

**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

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

The National Cable & Telecommunications Association (“NCTA”) hereby submits its Reply Comments in response to comments filed on the Second Further Notice of Proposed Rulemaking in this proceeding.<sup>1</sup>

**I. Constraining the Image of Non-Broadcast Programming**

As the Commission has recognized, the ability to constrain the image of high value digital content that could be output over unprotected analog component interfaces is a necessary tool for making such high value content available to MVPDs.<sup>2</sup> As long as the possibility exists for analog component interfaces to output HDTV content without constraint, MVPDs will be

---

<sup>1</sup> The Second Report and Order (“*Second R&O*”) and Second Further Notice of Proposed Rulemaking (“*2dFNPRM*”) and text of the Proposed Rules (“*Plug and Play Rules*”) were released together on October 9, 2003. *Implementation of Section 304 of the Telecommunications Act of 1996*, Second Report and Order and Second Further Notice of Proposed Rulemaking, 18 FCC Rcd 20885 (2003) The Media Bureau extended the comment date for the *2dFNPRM* to February 13, 2004 and the Reply Comment date to March 15, 2004. *Order*, DA 03-4085 (Dec. 23, 2003)

<sup>2</sup> *Second R&O*, 18 FCC Rcd at 20913, 20920 ( ¶¶ 64, 82).

handicapped in negotiating with programmers who are legitimately concerned about unauthorized redistribution of their high value programming. In December 2003, the cable and CE industries agreed upon the technology for implementing image constraint, independent of copy control state, thus setting the stage for marketplace dynamics between cable operators and program suppliers for optimizing the use (or non-use) of constrained image triggers (“CITs”).<sup>3</sup>

Other Comments support image constraint for non-broadcast programming and its implementation. MPAA explains that the use of image constraint will not reduce consumer options, but will facilitate greater consumer choice. As MPAA starkly puts it, consumers just won’t get an early release of “Movie X” on cable if there is no tool for constraining HD images that are output over unprotected component analog ports.<sup>4</sup> Some content providers believe—and some courts have agreed—that there is no inherent consumer right to make perfect digital copies.<sup>5</sup>

The other major MVPD industry competing for programming—represented by EchoStar, DirecTV, and its marketing partner BellSouth—agrees that image constraint is a necessary tool

---

<sup>3</sup> CEA and HRRC resuscitate a complaint raised in their status report of September 3, 2003 that the cable industry forced the constrained image trigger into the DFAST agreement. CEA Comments at 7-8; HRRC Comments at 1-2. The MOU specifically left it to the Commission to decide whether image constraint should be permitted on non-broadcast content. *Second R&O*, 18 FCC Rcd at 20912-13 (¶ 63). The Commission agreed with content providers and NCTA that it should, at least prior to a final FCC determination to the contrary, not prohibit “the inclusion of [CIT] functionality in devices” and noted that the DFAST agreement would need to address how to implement the image constraint capability. *Id.* at 20913 (¶ 64, n.171). The agreement was changed accordingly to incorporate the specific technology agreed to with CE. By contrast, the DFAST agreement was not changed at that time to require selectable output control, even though the Second Report & Order recognized that the capability was permitted and may be desirable. *Id.* at 20912 (¶ 61).

<sup>4</sup> MPAA Comments at 6.

<sup>5</sup> *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 459 (2d Cir. 2001) (“We know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original”); *United States v. Elcom*, 203 F. Supp. 2d 1111, 1131 (N.D.Cal. 2002) (citing to *Corley* decision). As DirecTV notes, content providers have rights, too, which must be balanced against possible inconveniences to customers. DirecTV Comments at 4-9.

for negotiating programming agreements with content providers and should be exercised in accordance with the applicable terms of negotiated programming agreements.<sup>6</sup>

Most importantly, the empirical information submitted confirms that the impact of image constraints on consumers with component analog ports should be minimal. MPAA explains that “image constraint would have no noticeable effect on [current] consumers, because current 1080i displays cannot fully resolve a 1080i signal, and as a result, a recorded constrained image will appear exactly the same as the original 1080i image on such displays.”<sup>7</sup> In addition, “older-model DVD recorders are incapable of recording 1080i content anyway, and thus the issue of image constraint is a moot point for such devices.”<sup>8</sup> DirecTV makes the same point—that an image “constrained” to 520,000 pixels is actually quite good, considering the actual resolution capabilities of the legacy equipment at issue.<sup>9</sup>

By contrast CERC and CEA advance no empirical evidence whatsoever of the actual impact on consumers, let alone whether it will be a negative impact. They estimate that 5.4

---

<sup>6</sup> EchoStar Comments at 4; DirecTV Comments at 6; BellSouth Comments at 3. DirecTV’s request that the FCC adopt a rule on implementation of image constraints in legacy DBS boxes is misplaced. DirecTV Comments at 7. DirecTV’s request is that ports be disabled where they cannot otherwise read and respect image constraints that may be required by their program suppliers. The FCC rules permit, but do not specify, image constraint tools. *Second R&O*, 18 FCC Rcd at 20913 (¶ 64). The specific application of copy protection and image constraint is normally negotiated in affiliation agreements. DirecTV’s request appears to be a request that the FCC specify by order that disabling a port will meet all programmers’ requirements for image constraint. The application of image constraint for particular programs should remain a negotiated term with content providers, rather than an FCC rule.

<sup>7</sup> MPAA Comments at 6. NCTA understands that during a DTV Roundtable meeting on Capitol Hill, MPAA staged a demonstration of image constrained HDTV content. The demonstrations took a broadcast-quality HDTV 1920 pixel by 1080-line master tape of the movie “Oceans Eleven” and the TV show “ER,” constrained the image to 960 pixels x 540 lines, and then upconverted this constrained image to the original 1920 x 1080 format. A JVC Digital VHS tape was made of this content by intercutting between the original unconstrained image and the upconverted constrained image. This tape was then played on a high-quality 38” Thomson direct view CRT monitor (which was representative of the current state of the art in legacy HDTV displays with analog HDTV only inputs). No one viewing the tape was able to discern the difference between the intercut images. At the round table meeting, MPAA challenged other HDTV monitor manufacturers to view this tape on their monitors but no one took MPAA up on the challenge.

<sup>8</sup> MPAA Comments at 7.

<sup>9</sup> DirecTV Comments at 6.

million TV's have been sold that "have been classified as capable of 'HDTV' resolution."<sup>10</sup> Noticeably, CEA puts "HDTV" in quotation marks. They do not describe the actual resolution capabilities of the actual sets—which are known to be less than 1080i.<sup>11</sup> They include in their count of 5.4 million all TVs taking feed from HD broadcast tuners, rather than cable or satellite set-top boxes. They do not discuss the recording capabilities of legacy DVRs.<sup>12</sup> Instead, they *assume* devastating impact; ask that cable and satellite *set-top boxes* (as distinct from the Unidirectional Digital Cable Products ("UDCPs") which they will be making) be banned from using image constraint; that all UDCP's be free to ignore image constraint signals while they network unprotected HD signals around the home; and that they be permitted to continue selling such unprotected devices into the market at the rate of one out of every four DTVs, exacerbating a problem of their own making.<sup>13</sup>

CEA and CERC ultimately attempt to portray this issue as one in which early adopters will be punished.<sup>14</sup> They ask the rhetorical question of what could have been done differently?<sup>15</sup> CEA members *could* have manufactured and sold devices with protected digital ports to avoid

---

<sup>10</sup> CEA Comments at 4.

<sup>11</sup> As noted in HRRC comments, CE Manufacturers also sold and continue to sell "enhanced definition" televisions with resolution of approximately 480p. HRRC Comments, Appendix A (Declaration of Sean Wargo) at ¶ 3. These sets are also incapable of fully resolving a HD signal, and would show no visible difference in a signal which had been subject to image constraint. CE manufacturers continue to build, and CE retailers continue to sell, such EDTVs.

<sup>12</sup> CEA Comments at 4-5. They also dispute, without anymore than saying it, that the notion that consumers will not be able to tell the difference between 1080i and image constrained programming is "anecdotal, false, unsupported in the record and counter to everyday experience." *Id.* at 5. Realizing that they have no proof for this rhetorical claim, they retreat to saying that those who purchase HD programming are entitled to "full capabilities" regardless of whether the programs reach the "full theoretical capabilities of each specification." *Id.* That retreat also begs the question of protecting the digital content.

<sup>13</sup> Public Knowledge claims that constraining the image of 1080i content reduces its size so that it could be more easily passed around on the Internet. Public Knowledge Comments at 5. What Public Knowledge ignores is that image constraint was developed as an acceptable tool for migrating toward protected digital interfaces, and that content providers have sufficient comfort in this technique to adopt it as one tool for addressing the analog hole. Public Knowledge's purported concern with protection of program content is merely an effort to keep the analog hole open.

<sup>14</sup> CEA Comments at 4-5, 6.

<sup>15</sup> CERC Comments at 2.

building a legacy analog hole. Unfortunately, they did not. But, fortunately, given the state of the art at the time and the record in this proceeding, image constraint presents no noticeable difference. The hole can be addressed and the consumer can still have high resolution images.

With respect to new devices, UDCP manufacturers have the option of including component analog ports with image constraint capability, and are permitted to use line doubling or other techniques to improve the perceived quality of an image constrained picture.<sup>16</sup> They may also include protected digital ports. This will create the market incentives to migrate customers to protected digital ports which will significantly advance the digital transition. As MPAA notes, “it seems unlikely, given the digital transition, that future DTV devices will be manufactured with only component analog outputs, unless it is part of a concerted effort to subvert digital content protection.”<sup>17</sup> 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 outputs.

With the CIT in place, program suppliers can determine whether or not to display full resolution programming through analog component outputs and assume the risk of unauthorized redistribution of re-digitized high resolution programming. Cable operators will be able to negotiate for content from those suppliers who require image constraint as well as those that do not. 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 image constraints. The Commission always remains able to address any actual concerns over implementation as may be necessary and within its authority. There is no basis for limiting the use of image constraints on non-broadcast programming at this time.

---

<sup>16</sup> NCTA Comments at 4-5, n.7.

<sup>17</sup> MPAA Comments at 6.

## II. Consumer Information Disclosures

In its initial Comments, NCTA explained the importance to consumers of having a full understanding of UDCPs in order to minimize the potential for confusion when they bring their new purchase home and connect it to a cable system. Consumers should understand when 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. Several parties, such as Public Knowledge, agree that more pre-sale information is desirable.<sup>18</sup>

The Home Recording Rights Coalition presents interesting testimony on this point. It says that “additional labeling requirements could get in the way” and are “likely to be confusing to customers.”<sup>19</sup> The HRRC specifically opposes any requirement to inform customers in advance of what a UDCP can *not* do. It notes that these devices will have DVI ports to which navigation devices (set-top boxes) may be added, so “there is little of which the consumer needs to be ‘warned’ before making a purchase decision.”<sup>20</sup> But advertising a UDCP as “digital cable ready” needs to mean more than that the TV can connect to a set-top box. There should be multiple paths for communicating the capabilities and limitations of UDCPs, including the cable industry’s educational efforts detailed in our initial Comments, the press, post-sale material, and pre-sale information provided by retailers. Retail labels routinely distinguish between 480p, 720p, and 1080i resolutions, effective viewing angles, on-screen menus, component video, S-video, DVI and other output connectors, internal HD tuners, and so forth. We assume that consumers make purchase decisions based upon comparisons of such information for competing products.

---

<sup>18</sup> Public Knowledge Comments at 7.

<sup>19</sup> HRRC Comments at 12-13.

<sup>20</sup> *Id.* at 13.

Retailers should be informing customers that *unidirectional* “digital cable ready” devices do not have the necessary interactive functionality to, for example, order video-on-demand movies or other interactive services on their own. Consumers will be better informed if they know, at point of purchase, that the digital television can receive basic analog, digital basic and digital premium cable television; that a CableCARD provided by the local cable operator is required to view encrypted digital programming; and that certain advanced interactive digital cable services such as video-on-demand, cable operator enhanced program guide, and data enhanced television service may still require the use of a set-top box.

CERC opposes mandatory pre-sale labeling, but indicates that its member retailers will be providing some pre-sale information to consumers by way of a “simple communication,” although CERC does not say whether they will inform customers of UDCPs’ two-way limitations.<sup>21</sup> CERC should inform the Commission of what its members will tell customers about the capabilities and limitations of these UDCPs.

### **III. Applying Digital Transmission Standards to Smaller Systems**

In its initial Comments, NCTA noted that the economics of smaller systems would be strained if subjected to the headend and transmission standards applied to systems with an activated channel capacity of 750 MHz.<sup>22</sup> CEA agrees, noting that in the due course of rebuilds, these systems will naturally become subject to the agreed-upon standards.<sup>23</sup> As in the first round of comments in 2003, no party has advocated extending the standards to 550 MHz systems. Matsushita suggests that the Commission conduct a “study” of how many systems are 750 MHz,

---

<sup>21</sup> CERC Comments at 4. Indeed, CERC believes customers will not even understand what “interactive” means and get confused if they see the term on a label. *Id.* This is all the more reason to have detailed information available pre-sale.

<sup>22</sup> NCTA Comments at 6.

<sup>23</sup> CEA Comments at 11-12.

but that information has already been submitted in the record: 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,<sup>24</sup> quite sufficient to sustain a national market in UDCP compliant retail equipment. The Commission should 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**

##### **A. Why CableLabs Is The Natural Candidate for Approving Outputs and Security Technologies**

In its initial comments, NCTA detailed why CableLabs is the natural authority for serving as one of two paths for approval of output and content protection technologies in UDCPs and we listed a number of draft criteria CableLabs would employ in any review process.<sup>25</sup> The proper operation of new outputs or new security techniques is vital to cable operators’ core business. 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.

As also explained, CableLabs is not the “sole initial arbiter” of approved technologies. Any decision by CableLabs is subject to appeal to the FCC.<sup>26</sup> Moreover, the applicable

---

<sup>24</sup> Compare Matsushita Comments at 2 with NCTA 2003 Year-End Industry Overview, at 2, 20 (available online at [http://www.ncta.com/pdf\\_files/Overview.pdf](http://www.ncta.com/pdf_files/Overview.pdf)).

<sup>25</sup> The details of CableLabs’ pivotal role and success in advancing the digital transition are set forth in NCTA Comments at 7-19. CableLabs is a world-respected laboratory with an enviable track record in drafting widely adopted specifications, testing and certifying multiple types of equipment, engaging with over 500 companies, enabling innovation, and promoting market entry by competitive CE manufacturers well before any FCC “retail availability” requirements were adopted.

<sup>26</sup> NCTA Comments at 14-15.

agreements specifically create a parallel, independent path for program suppliers to approve new content protection technologies which will then be “deemed approved” by CableLabs.<sup>27</sup>

CableLabs’ role in this process is supported by the actual manufacturers seeking to build into this market: CEA supports it on behalf of its members,<sup>28</sup> as does Philips and Matsushita in individual comments.<sup>29</sup> CableLabs’ role is also supported by the principal content providers: through MPAA, the suppliers of high value digital content are willing to trust CableLabs to maintain network security and the tools essential for cable operators to obtain high value programming and provide reasonable assurance that such content will be protected from unauthorized access.

**B. DBS Remains Free to Define, Buy and Build Security and Outputs Without CableLabs or Any Approval**

The opposition of the DBS industry—through EchoStar, DirecTV, and its marketing partner BellSouth—appears to be rooted in a factual misunderstanding of what CableLabs will be approving. DirecTV appears to believe that CableLabs’ approval is required for new

---

<sup>27</sup> *Id.* at 15.

<sup>28</sup> CEA Comments at 13. CEA and HRRC are advocating self-certification of outputs and content protection for flag protection only. CEA Comments at 15; HRRC Comments at 11. However, as the manufacturers and content owners realize, Table A approvals do not automatically qualify for UDCP approval. NCTA Comments at 19-21. CEA, MPAA, the Digital Transmission Licensing Administrator, LLC (“DTLA”), Microsoft, Philips, Matsushita, Public Knowledge, and others agree that the two regimes should not be unified. IT Industry Comments at 7-8; CEA Flag Comments at 4; MPAA Flag Comments at 3; DTLA Flag Comments at 13-14; IT Coalition Flag Comments at 14-15; Philips Flag Comments at 29-30; Matsushita Flag Comments at 1-2; Public Knowledge Flag Comments at 17. AAI advocates merging the regimes but with a profound misunderstanding of the differences in flag and MVPD content. AAI Comments at 3-4.

<sup>29</sup> Philips Comments at 3-4; Matsushita Comments at 3. HRRC claims that CableLabs is the only UDCP test facility. HRRC Comments at 9-10. There are actually many testing and development facilities that may be helpful in this process. Those currently known to us are posted at <http://www.opencable.com/testing/testing.html> (testing) and <http://www.opencable.com/testing/support.html> (development support). MSOs have also offered to co-establish more in cooperation with CEA. The MOU also includes a commitment by MSOs to assist CE manufacturers in buying their own head-ends for development, as many have, and in making CableLabs available for development support, as it is. Memorandum of Understanding, ¶ 3.9.4, 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”).

interfaces on *DirecTV's* set-top boxes.<sup>30</sup> In fact, CableLabs' role relates to UDCP devices that connect to cable networks and use the POD-Host interface under the DFAST license. The DFAST license defines only the mechanism for effectuating the POD-Host interface—an interface that is not applicable to DirecTV receivers and which has no bearing on its distribution of its services or operation of its uplink or proprietary set-top boxes.

Indeed, Mr. Murdoch has explained in detail DirecTV's ability to manufacture equipment in-house, and to dictate all specifications on DirecTV set-top boxes to assure his ability to pursue competitive product launches with only his proprietary set-top boxes.<sup>31</sup> DirecTV may build or contract for any outputs it desires. Thus, CableLabs will not be defining technology for DBS. DirecTV and EchoStar can continue to write the specifications for their equipment, make the equipment themselves, and negotiate with content providers over the digital outputs that are acceptable under programming agreements, as DirecTV requests. Indeed, the DBS industry has considerably more freedom in this area than cable does. CableLabs cannot approve or disapprove new UDCP outputs or content protection technologies without a detailed process and appeal to the FCC. EchoStar and DirecTV can simply write a specification or issue a purchase order.

### **C. Standards and Approaches**

Several parties have submitted proposals for the actual standards and procedures for approving outputs and content protection technologies, both in this docket and the “broadcast

---

<sup>30</sup> Further Comments of DirecTV, Inc. at 10-11 (filed Feb. 13, 2004).

<sup>31</sup> *Murdoch Outlines DirecTV's Future*, Satellite Business News (Dec. 31, 2003) (“Our main move is to have one box, which EchoStar has. One box which we will design, albeit with the best brains we can find from all these companies. And we will put that out to tender. And eventually, we'd like that box to become the same box that goes to Latin America, North America, and even other parts of the world, so we can get all the possible benefits of mass manufacturing . . . . Our greatest worry is that there are about 120 different DirecTV boxes out in the market today. And we have to work through that with churn and things, so there's as few legacy boxes as possible in three or four years time. So, when we advertise a great new service, it may only be possible for that to come through one of these new boxes.”)

flag” docket. In NCTA’s view, the first lesson from the comments is that output and content protection review criteria are benefiting from more thought, more discussion and less rhetoric. For example, Microsoft has already improved its proposed approach by addressing one key area—standards for licensing approved technologies under RAND or reasonable non-asserts—on which it had been silent last year.<sup>32</sup> Thus, by waiting only a few months, the Commission has benefited from improvements in proposals. Some parties (*e.g.*, DTLA) have candidly said they would rather wait and see what others came up with, and build or respond from there.<sup>33</sup>

Attached as Exhibit A is NCTA’s summary of where the various proposals to date – including the criteria NCTA listed that might be employed by CableLabs – now stand in comparison with each other. The variations in supposedly “objective” and “functional” words and phrases offered by other comments are pregnant with attempts to skew the outcome towards specific and often proprietary outcomes. For example, Microsoft and Intel offer a proposal that would favor pure software solutions that can be implemented far more readily in PCs than in retail CE products, which rely more on hardware.<sup>34</sup> Philips points out (in broadcast flag comments), that the interim review criteria the FCC adopted from the MS-HP 2003 filing seem to compel authentication, which is only used in encryption-based systems.<sup>35</sup>

Most proposals overlook some crucial fundamentals such as the ability of the technology to actually transport video from cable to the consumer, or to deliver the cable services for which the UDCP is actually licensed. The comparison—and the drawbacks of the various proposals—

---

<sup>32</sup> Microsoft Comments at 12-13. The American Antitrust Institute claims that the Microsoft-HP proposal of 2003 is the “only way” to approach the issue. AAI Comments at 4. In 2004, even Microsoft does not claim that, indicating it will “build upon” that proposal. Microsoft Comments at 10.

<sup>33</sup> DTLA Flag Comments at 7.

<sup>34</sup> Microsoft Comments at 9; Intel Comments at 4-5.

<sup>35</sup> Microsoft *ex parte* letter, dated August 8, 2003 (“August 8 *ex parte*”); Philips Flag Comments at 8-10, 18. Philips also proposes watermarking or fingerprinting as an alternative to encryption-based authentication content protection. *Id.*

can best be evaluated by considering how each addresses: (1) Security Interfaces, Security Processing, New Algorithms and Points of Attack; (2) the Effectiveness of the Technology; (3) Revocation and Renewability; (4) Licensing Terms; (5) Video Transport; (6) Consistency of the Proposal with the DFAST License and the Joint Test Suite; (7) Burden on the Cable Operator; and (8) Relationship to the Broadcast Flag. The various proposals are summarized in Exhibit A.

1. **Security Interfaces.** Some proposals would limit permitted outputs and content protection technologies to public standard algorithms.<sup>36</sup> Others would allow proprietary solutions, which might or might not be interoperable or that have not (yet) been standardized. By separate filings, Microsoft/HP/Dell/Apple (“Microsoft”) and Intel have submitted proposals that appear neutral in language but are, as DTLA points out, heavily biased to software-only solutions.<sup>37</sup> Both ask that “a content protection method may be implemented in software or hardware or in any combination of the two.”<sup>38</sup> Both require interoperability, so that content may be “transmitted among or recorded by a variety of consumer devices, including but not limited to single and multi-function devices such as TVs, set-top boxes, game consoles and personal video recorders as well as general purpose devices such as PCs.”<sup>39</sup> Microsoft asks for a “consistent consumer experience,” so that there will be reduced consumer “confusion” about what can be copied from various platforms.<sup>40</sup> That may define DRM, but it does not describe (today) content protection and secure 1394/5C digital interfaces trying to connect to a wireless network.

Both require that the CP technology be upgradeable and renewable, which may be true for PC software, but may be more challenging for CE devices that do not have an upstream

---

<sup>36</sup> *E.g.*, Genesis Comments at 4-5; Philips Comments at 15. DTLA rejects this contention. DTLA comments at 9.

<sup>37</sup> DTLA Flag Comments at 14.

<sup>38</sup> Microsoft Comments at 8, 9; Intel Comments at 4.

<sup>39</sup> Intel Comments at 4; Microsoft Comments at 8.

<sup>40</sup> Microsoft Comments at 3-4.

cable connection and have device certificates hardwired into the circuitry. Microsoft's proposal from last year would have set percentage guidelines of what processing power could be used for an encryption algorithm, which would have nicely fit PCs but not all retail CE devices.<sup>41</sup> While IT interests try to steer the outcome to pure software protection, major content providers inform us that they are not yet convinced that pure software protection is sufficient for protection of high-value programming on cable networks.

2. **Effectiveness.** For as much detail as may appear to be within the Microsoft/HP/Dell/Apple and Intel proposals, they are substantially silent on a key point: how "effective" does the technology have to be in protecting content? The IT interests do not say. As MPAA properly points out, this does nothing to define substantive levels of protection in authentication. It would allow encrypted P2P as an approved content protection technology. MPAA suggests benchmarking to DTCP, while even DTLA (the administrator of DTCP) is rightly concerned that any benchmark needs to leave room for innovation.<sup>42</sup>

Robustness requirements, ordinarily found in license agreements, are also a subject of disagreement among the commenters. Microsoft/HP/Dell/Apple and Intel propose reducing robustness to an ordinary user standard, even for UDCPs.<sup>43</sup> This would significantly reduce the level of protection required by DFAST. The reason for the request, we believe, is because of the vulnerability of user accessible buses. The vulnerability of graphics buses, for example, is debatable. Microsoft would ask that the rules presume they are inaccessible, but they are

---

<sup>41</sup> Microsoft-HP proposed that implementing the encryption algorithm in hardware should use less than 10% of digital logic; and that in software, it should use less than 3% of the processing power used to produce the baseband video signal. August 8 *ex parte* at 7.

<sup>42</sup> MPAA Comments at 2, note 2; DTLA Flag Comments at 4, 7, 9.

<sup>43</sup> Microsoft Comments at 8, 13.

designed to be accessible for the upgrade of video cards.<sup>44</sup> With the use of an inexpensive “frame grabber,” sophisticated users can easily retrieve video images, frame-by-frame, in the clear as the bus is the last place before in-the-clear images pass on the way to the CRT. Unless and until encryptions for removable video cards (like CableCARDS) are developed, the bus presents an insecure location and unless robustness is set at the professional level, will provide easy access to unencrypted unencoded video.

Microsoft’s approach is best summed up in its announcement that “PC owners should not have to sacrifice (or lose some of the efficiency of) those functions merely because their PC is capable of receiving content over cable, nor should technologies developed for PCs be excluded from use in digital cable devices solely because the PCs perform additional functions.”<sup>45</sup> If there were no need to have a secure cable network, that might be true. But building a secure and robust copy protection technology into a PC, which is designed to be user accessible and to share content across applications and the Internet, is not an easy task and not one that should be assumed as “finished” in an FCC rule.

**3. License.** Intel takes one extreme—that there should be no review of license terms at all. “The Commission should not, however, interfere with the private right to contract by dictating the terms and conditions of private license agreements, or otherwise even require the licensing of any proprietary technology. Those decisions should all be left to private parties in

---

<sup>44</sup> In its August 8 *ex parte*, Microsoft argues that although buses are part of a PC’s “open architecture,” the buses are not *per se* “unable to protect the security of content.” August 8 *ex parte* at 6. Indeed, Microsoft says that the PC industry has developed technologies “proven effective in the marketplace” to protect content in the open areas of PCs, but these technologies are neither identified nor explained. *Id.* DTLA says no clear compressed video should be available on a user accessible bus. DTLA Comments at 9. In Microsoft’s 2004 proposal, it simply seeks to define all graphics buses as not “user accessible,” which not even Intel proposes.

<sup>45</sup> Microsoft Comments at 11.

the market place.”<sup>46</sup> Others express concern that a patented technology installed in UDCPs could expose third parties to unexpected, uncontrolled license fees.<sup>47</sup> They argue that undisclosed patent claims might later subject deployed equipment to serious liability or to recall (as the FTC believed had occurred with Rambus and Unocal).<sup>48</sup>

Comments have suggested a wide array of substantive license terms the FCC should compel: mandatory RAND; a limitation on “unreasonable” patent non-asserts; no insistence on control of downstream devices or outputs from a sink; a required role for content providers in change management of the technology; and a required role for patent licensees in changes by the patent holder in licensed applications.<sup>49</sup> These license terms are usually subject to vigorous debate and negotiation, rather than being set in advance by the government.

MPAA raises the legitimate point that new outputs should not be forced on unwilling parties. It observes that by requiring selectable output control for all outputs, new ports and new content protection technologies could be approved for those who want them, and are willing to pay the license fees, but could be turned off for those who do not. It concludes that this would allow the market in new technologies to operate more fluidly.<sup>50</sup>

---

<sup>46</sup> Intel Comments at 4.

<sup>47</sup> Time Warner Comments at 14-15. Macrovision, for example, imposes a content-based fee upstream from the device that includes it.  
[http://www.macrovision.com/partners/entertainment/become\\_a\\_licensee/How\\_to\\_Obtain\\_Macrovision\\_License.pdf](http://www.macrovision.com/partners/entertainment/become_a_licensee/How_to_Obtain_Macrovision_License.pdf)

<sup>48</sup> <http://www.ftc.gov/opa/2002/06/rambus.htm>; <http://www.ftc.gov/opa/2004/02/rambusdecision.htm>.

*See also* <http://www.ftc.gov/opa/2003/03/unocal.htm>.

<sup>49</sup> *E.g.*, Philips Comments at 6; Genesis Comments at 6-8; *See also* DTLA Flag Comments at 12.

<sup>50</sup> MPAA Comments at 4. CEA finds “irony” in a digital transition path which would use image constraint to motivate consumers to adopt protected digital ports, but then permit selectable output control to turn off those ports. CEA Comments at 5-6. But whatever one’s position on selectable output control, there plainly do exist potential benefits from using selectable output control in providing new product to consumers, in protecting against seriously compromised ports (without necessarily disabling the entire device), or in preventing inordinate royalties and liabilities from accruing to content providers and MVPDs.

4. **Relationship of UDCP Approval to the Broadcast Flag.** For some parties, approval of a technology for use in implementing the broadcast flag means it should be suitable for content protection over cable. American Antitrust Institute, for example, claims that approval for one is approval for all, regardless of the “mode of delivery,” and that it is a burden to seek approval of a technology under both regimes.<sup>51</sup>

NCTA has previously explained that approval under the broadcast flag environment is insufficient to automatically qualify for approval of a technology for a UDCP, because they operate in different regimes (e.g., one encrypted and secure, the other free, in-the-clear, over-the-air) with different functional requirements (e.g., one with copy protection, the other without).<sup>52</sup> CEA, MPAA, Public Knowledge, and Matsushita, among others, agreed.<sup>53</sup> Content providers, too, make clear that security may need to be separately evaluated depending on physical layer and form factor. In the 5C license, for example, content providers distinguish between the mapping of DTCP to certain connectors (USB, MOST, Home PNA, PCI, Bluetooth, Home RF and 802.11), and others (e.g., Ethernet).<sup>54</sup> Approval of a content protection technology over one form may not be the same thing as approval over another.<sup>55</sup>

5. **Video Transport.** It is significant what all of these other proposals neglect: the cable issues. It is fine to say, for example, that DTCP is now mapped to USB, but there is as yet no clear definition for video transport using that output with DTCP. Can a technology secure

---

<sup>51</sup> AAI Comments at 3-4. Genesis and Philips also take this approach. Genesis Comments at 8-10; Philips Comments at 6.

<sup>52</sup> NCTA Comments at 19-21.

<sup>53</sup> See Comments cited in footnote 28.

<sup>54</sup> Content Participant Agreement: Audiovisual Version, § 3.7 (pp. 14-15).

<sup>55</sup> Intel and Matsushita claim that DTCP works over everything. “DTCP-IP delivers the same level of content protection, including the same level of compliance and robustness, as does DTCP over IEEE 1394.” Intel Comments at 6. See also Matsushita Comments at 4. Unfortunately, the video transport is poorly defined, and the claim needs to be proven out. Rulemaking comments don’t obviate the need for empirical proof.

video so effectively that it does not even transport it? The navigation device rules are supposed to address retail availability of devices that deliver cable service from cable systems to cable customers. CableLabs is the only party which has even posed the question: Is the video transport method clearly defined?

6. **DFAST/JTS Consistency.** Another area neglected in all of these other proposals is whether the technology interferes with a UDCP's obligations under the rest of the rules and agreements, including the Joint Test Suite ("JTS") agreed upon by the parties to the MOU. Under DFAST, "no feature or functionality of a UDCP, as manufactured and distributed, shall (a) technically disrupt, impede or impair the delivery of services to a cable customer; (b) cause physical harm to the network or the POD; (c) facilitate theft of service or otherwise interfere with reasonable actions taken by Cable Operators to prevent theft of service; (d) jeopardize the security of any services offered over the cable system; or (e) interfere with or disable the ability of a Cable Operator to communicate with or disable a POD Module or to disable services being transmitted through a POD Module."<sup>56</sup>

A new output or content protection technology must not prevent a UDCP from meeting these standards. For example, suppose a new copy protection system is developed to work with a CableCARD-enabled 802.11B wireless gateway device with robustness and compliance rules that are consistent with the encryption scheme. The system may well pass standard definition television signals. However, that interface is inherently limited to a maximum throughput of 10 Mbps, which works fine for most SDTV formats, but will fail when trying to tune an HDTV service. The proposed output cannot satisfy the existing requirements of the JTS because it would technically impede the delivery of services to a cable customer.

---

<sup>56</sup> DFAST License Agreement, ¶ 2.2, available at FNPRM, 18 FCC Rcd at 576.

It would be imprudent to approve an output or content protection technology that would disrupt service. CableLabs is the only party which has even asked whether the proposed output/technology would interfere with a UDCP device's meeting its DFAST or testing obligations.

7. **Burden on the Cable Network.** The Plug and Play Rules and the MOU have an agreed set of standards upon which a retail market in UDCPs can operate. Many content protection technologies include certificate revocation lists ("CRLs"), system renewability messages ("SRMs"), and other communications intended to facilitate the operation of the technology. But it is not a given that CRLs or SRMs will be automatically transported on every delivery platform. They might be loaded onto DVDs; they might be downloaded over the Internet; they might be carried on cable. There should be no assumption that cable operators will add new functionalities to their headends to support every new output, every new CP technology, and every new CRL or SRM.

In 5C, content providers specifically provided that they were under no obligation to obtain cable carriage of CRLs.<sup>57</sup> Under the MOU, the design of UDCP products may not impose additional investment requirements on the cable distribution network, beyond the MSO obligations specifically undertaken.<sup>58</sup> CableLabs is the only party that asked the question: Are there operational burdens placed on MSOs and other content distributors? Are the Revocation and Renewability solutions easily adapted by an MSO so it can use Selective Denial of Service?

---

<sup>57</sup> Content Participant Agreement: Audiovisual Version, § 6.2 (p. 29).

<sup>58</sup> MOU ¶ 3.12, *available at FNPRM*, 18 FCC Rcd at 547 (1997).

#### **D. The CableLabs Approach**

Against this backdrop, the Commission can see that the criteria proposed by CableLabs and cited in NCTA's initial comments strike a sensible middle ground.

##### **1. Security Interfaces/ Security Processing/New Algorithms/Points of Attack.**

As is evident from Exhibit A, the questions posed by CableLabs require evaluation of the same general security elements addressed by the other proposals, but with these benefits:

- They are based upon and written by security professionals for use by security professionals.
- They are more defined in the questions asked.
- They do not limit output and content protection to those that pass through a standards body. This could facilitate innovation with connectors that have not (yet) been standardized.
- They do call for a specific discussion of interoperability, which is needed to satisfy customer expectations and DFAST.
- They do not “discriminate” against PCs. They do ask fair questions about the effectiveness of security and robustness across any platform, whether a CE DTV or a PC.

**2. Effectiveness.** The CableLabs criteria ask the key question about the effectiveness of the technology, but allow for judgments to be made about tradeoffs made for security versus cost. It is important to note that no-one submitting comments—indeed, not even the Commission—knows the “right” answers to every question for every technology today. The proposals will vary. The specific engineering tradeoffs for protection technologies can vary widely. Trying to set the answers in advance in an FCC rule would be a mistake. We agree with Intel that “there simply is no one size fits all formulation.”<sup>59</sup> By allowing this balancing to

---

<sup>59</sup> Intel Comments at 3.

continue going forward, it avoids locking in DTCP as the only permissible standard. We agree with EchoStar<sup>60</sup> there should be confidentiality protections, and CableLabs has them.

CableLabs is an essential part of this process. The fact that CableLabs has a commitment to maintaining a network secure enough to retain and attract new content for cable subscribers is an asset. By allowing the initial judgment to be exercised by CableLabs (subject to FCC review<sup>61</sup>), the Commission can use the market interplay between content providers, distributors, and proponents of new technology to strike optimal outcomes.<sup>62</sup>

**3. Licensing Terms.** The CableLabs criteria address the myriad concerns over licensing raised by the parties. There should be review of license terms, which includes review of disclosed patents.<sup>63</sup> It is possible, as Philips argues, that FCC judgments about license terms in the flag context might help inform proper license terms for other technologies. But we do not think it a proper role for the FCC to prescribe in advance the patent license terms for all technologies.<sup>64</sup> The CableLabs questions clearly seek to encourage RAND, but they do not prohibit non-asserts, nor do they prescribe the amount of any license fee.

We agree with Time Warner that the Commission should take this a step further. There should be no royalties for content protection technologies unless the technology is voluntarily chosen by a content provider or cable operator. In this regard, MPAA notes that selectable

---

<sup>60</sup> EchoStar Comments at 5-6.

<sup>61</sup> FCC review will be expeditious as opposed to a proposal for intermediate arbitration. *See* MPAA Comments at 2, 4.

<sup>62</sup> HRRC seems to suggest that except for unidirectional UDCPs CableLabs should not review technologies. HRRC Comments at 10-11. In fact, the complexity of interactive devices and the potential for harm from upstream path would require even more careful review. This is the subject of negotiation in the cable-CE bi-directional discussions, and is not appropriate for disposition in this present rulemaking.

<sup>63</sup> Time Warner Comments at 15; Genesis Comments at 4, 5 (n.12). As NCTA has previously submitted, the patent disclosure regimes used in approving existing connectors are reasonable and sufficient.

<sup>64</sup> Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service, 6 FCC Rcd 7024, 7034 (1991).

output control can be an effective tool for enforcing this approach, rather than having the government attempt to regulate the amount of royalties that are reasonable for technologies yet to be introduced.

4. **Relationship to Broadcast Flag.** As explained in our initial comments, approval of an output or content protection technology for UDCP use should automatically be approval for use in implementing the broadcast flag, but not vice versa. MPAA, Microsoft, Matsushita, DTLA, Public Knowledge, and others agree.<sup>65</sup>

5. **Video Transport.** This proceeding is supposed to address retail availability of devices that deliver cable service from cable systems to cable customers. Cable systems operate as competitive service providers. Retail devices are supposed to deliver those services as intended to be rendered by the service provider. CableLabs is the only party which has even posed the right questions about this foundational requirement for any technology used in UDCPs.

6. **DFAST/JTS Consistency.** CableLabs is the only party which has posed the right questions about whether the technology interferes with a UDCP's obligations under the plug and play rules and cable MSO-CE manufacturer agreements.

7. **Burden on the Cable Network.** As noted above, some outputs and content protection technologies rely upon other parties to make them work. For example, a revocable security technique may require propagation of a certificate revocation list ("CRL") from some source to the secure device. Today, there are a variety of methods of propagating such lists, and there is no assumption that any one method will always be available. This is why, for example, the 5C license<sup>66</sup> provides that content participants need not require their licensees (e.g., MVPDs)

---

<sup>65</sup> See Comments cited in footnote 28.

<sup>66</sup> Content Participant Agreement: Audiovisual Version, § 6.2 (p. 29).

to carry certificate revocation lists. Content protection technologies can be designed in ways that do not impose such burdens.

It is unrealistic to expect every MVPD to propagate every variety of CRL for every content protection technique, or to undertake any other investment at the headend that might facilitate a particular technique. It is also inconsistent with the MOU, which specifically provided that there should be no additional investment requirements on the cable distribution network, beyond the (substantial) MSO obligations specifically undertaken.<sup>67</sup> CableLabs is the only party which has posed the right questions about imposing additional obligations on the headend, in order to assess their feasibility.

#### **E. Why CableLabs is Preferable to an Inter-industry Panel or Self-Certification**

The diversity of suggested approaches to output review does not just reflect efforts by some proponents to skew the outcome in particular directions. It also reflects that there is much to learn in this new and rapidly evolving arena. It is understandable that many parties desire a fixed standard against which all content protection techniques can be measured, perhaps with enough certainty that self-certification would be possible. But there is nothing in the record supporting an industry consensus around any one answer. Should the Commission decide that only a secure key exchange is effective? Should all content protection technologies be revocable? How quickly must revocation lists propagate? Is the Commission prepared to declare that pure software solutions are ready to be relied upon without robustness in hardware—when the content community is not yet prepared to take that step across all platforms? What is the optimal tradeoff between security and cost?

---

<sup>67</sup> MOU ¶ 3.12, *available at FNPRM*, 18 FCC Rcd at 547.

It is quite simply premature to establish fixed criteria and fixed answers. Any efforts to decide the answers today will create significant risk that the answers will skew the market in one direction or another, or that the “bar” is lowered so far as to jeopardize the security of cable networks. Following the specific criteria developed by CableLabs allows the right questions to be asked in the forum agreed to in the MOU, with full review by the FCC. This process will allow all parties to benefit from actual experience, rather than trying to decide all the answers today.

Several parties have called for an inter-industry body, usually populated by representatives of the commenting party. That would include DBS, for example, approving cable outputs.<sup>68</sup> It is worth recalling that this process concerns outputs and content protection technologies on UDCPs that attach to cable systems. At present, 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. Any other party can also appeal a grant or denial to the FCC. However, it makes little sense to grant, for example, DBS or IT the right to block approval of a new cable connector, when DBS or IT can manufacturer or buy whatever connectors they want. That would merely create a choke point in which any interested party (e.g., competitors) could veto a new cable port while they installed one of their own.

It would be especially harmful to jump immediately to self-certification, as advocated by some parties, such as ATI and Intel.<sup>69</sup> Self-certification of content protection technologies

---

<sup>68</sup> DirecTV Comments at 11; EchoStar Comments at 4; BellSouth Comments at 4; AAI Comments at 5-6.

<sup>69</sup> ATI Comments at 4; Intel Comments at 6-7. To see where “self-certified” output and content protection technologies take us, one need only look at the comments of Intel and the American Antitrust Institute. Intel seeks to transform cable into a pure common carrier model. The American Antitrust Institute proposal also illustrates its goal for cable: pure common carriage, with no business model except transport, no security, no tiers, and no on-

provides no assurance that the technology will actually operate properly to deliver secure cable services. It may fail to actually deliver cable service as anticipated by the MOU, the agreed upon Joint Test Suite, FCC rules, and the navigation devices statute. An output may in reality be or become insecure. Indeed, insecurity appears to be a desired *feature*, as far as consumers see it, and one manufacturer or another will sell to it. For example, many manufacturers ignore Macrovision, which is required by the DMCA. Some DVD manufacturers have begun to exploit unprotected VGA ports to bypass copy protection.<sup>70</sup>

The MOU and current rules were developed against this real world backdrop, and assigned a specific role to CableLabs as an essential advance review. As the Commission knows, certification testing is common in the technology sector.<sup>71</sup> We know revocation will be subject to significant objections, delays, and even request for permanent grandfathering of compromised outputs, as discussed below. Self-certification presents a serious risk of opening a digital hole, followed by another round of pleas by manufacturers for mercy on “early adopters” of “legacy” devices that will only work with that digital hole open. We have the opportunity to review outputs and content protection technologies carefully and properly, with full rights of

---

demand. AAI Comments at 3-4, 5-6. This, however, is prohibited by the Cable Act. 47 U.S.C. § 541(c) (“Any cable system shall not be subject to regulation as a common carrier or utility by reason of providing any cable service.”). We are also at a loss to understand how their proposals comport with the constitutional protections of the cable television business. “Cable programmers and cable operators engage in and transmit speech, and they are entitled to the protection of the speech and press provisions of the First Amendment.” *Turner Broadcasting System v. FCC*, 512 U.S. 622, 636 (1994).

<sup>70</sup> “Coby DVD Deck Is Found To Beat Copy Protection Through Rare VGA-Out,” *Consumer Electronics Daily*, Jan. 2, 2004 at 2-3. *See also* “Dolby CES Crackdown Nets 61 Companies Peddling Unlicensed DVD Decks,” *Electronics Daily*, Jan. 28, 2004 at 2 (example of manufacturers’ ignoring licensing requirements). Amazingly, Intel also believes that, despite the well-known and widespread compromise of CSS, that it still provides “sufficient content protection.” Intel Comments at 7.

<sup>71</sup> *See* NCTA Reply Comments at 23-24 (filed April 28, 2003).

review at the FCC. Self-certification of outputs and content protection technologies may have its time, but that time is not today.<sup>72</sup>

The Commission should stay the course and 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.

#### **F. Revocation**

In its initial Comments, NCTA explained that how revocation is handled 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 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.

CERC and CEA seek a rule under which no device certificate would ever be revoked, with a fall back plea that they never be revoked “retroactively” for compromised interfaces or technologies.<sup>73</sup> The theory is that except for customers who have knowingly loaded cloned, lost or stolen certificates into their devices, the “consumer has done nothing wrong.” Translated, CEA/CERC’s position means that component analog with no protection will never close, and compromised digital ports will never close. MPAA rightly says this is not an option.<sup>74</sup>

---

<sup>72</sup> In this sense, we agree with Philip’s comments in the broadcast flag proceeding: We should first develop functional criteria for application by someone other than the proponent and prove they work before we consider transitioning to self-certification. Philips Flag Comments at 10-11.

<sup>73</sup> CERC Comments at 3-4; CEA Comments at 8-9. *See also* HRRC Comments at 7-9.

<sup>74</sup> MPAA Comments at 4.

In reality, CEA/CERC’s question about whether the customer “did wrong” is not the right question. Consumers will buy what manufacturers build, and one manufacturer or another will exploit every deficiency in protection technologies. Defects, non-compliance, and compromised technologies need to be addressed in the real world if secure networks are to remain secure, and cable networks will continue to deliver content that makes consumers want to buy “cable ready” devices. That DVDs keep being released when CSS is compromised is repeated ad nauseam by advocates of permanent grandfathering of compromised technology. But CSS should not set the standard for security of high value content on secure networks—nor may it under the law.<sup>75</sup>

Matsushita writes that cable operators can always use service denial, rather than revocation. To adopt that premise as a justification for grandfathering insecure ports is an open invitation to manufacture ports known to be insecure, and then assign the blame to cable when services are denied. Microsoft, HP, Dell and Apple collectively contend that revocation should only be considered after attempts have failed to modify all cable headends, and after software and firmware downloads from all headends have failed to “fix” compromised devices. Both seek to shift to cable operators all costs of “fixing” compromised outputs from UDCPs. Neither takes appropriate ownership of the responsibilities owed by manufacturers to their customers.

NCTA agrees that there needs to be consideration prior to revocation that accounts for all interests. Similar mechanisms—consultation between CableLabs and CE manufacturers, and consideration of alternative solutions—are already built into the DFAST license as a precondition to exercising certain remedies for material breach. But we do not believe that the

---

<sup>75</sup> Section 629(b) expressly requires that the Commission not jeopardize system security or impede the ability to identify and prevent theft of service. 47 U.S.C. § 549(b). HRRC argues that Section 629 is just about competition, with Congress “injecting” competition into the set-top box market and that promotion of competition is the “core” of this proceeding. HRRC Comments at 11. HRRC conspicuously ignores the other provisions of Section 629 such as protecting system security, which is the foundation of the cable business, and assuring the delivery of cable services. Clearly, Congress had considerably more in mind than just permitting retail sales of devices.

tools of revocation, or the mechanism for evaluating these interests, are identical in every case. There are already revocation and remedy clauses and procedures associated with DTCP and HDCP, to which device manufacturers have agreed. As new outputs and new content protection technologies are evaluated, so should be the means appropriate to that technology to handle revocation and renewal. Revocation criteria should not be set in advance.<sup>76</sup>

## V. Other issues

A few parties raise other issues extraneous to the matters at issue in these comments. Matsushita raises the question of whether separated security should be banned in 2006.<sup>77</sup> DirecTV raises issues concerning implementation of CGMS-A.<sup>78</sup> Neither is germane here. DirecTV repeats the concerns of its Petition for Reconsideration that Internet and IP delivered by cable are not covered by the current encoding rules. This has been effectively rebutted by NCTA and by BellSouth in response to that Petition.<sup>79</sup> Microsoft contends that the FCC should change the PICs, the JTS, and the rules to allow PCs to deliver the “functionality” of UDCPs without having to meet their compliance, robustness and testing standards.<sup>80</sup> We note that the cable and CE industries have submitted a proposed change in rules that would accommodate alternative test suites.<sup>81</sup> Microsoft’s other requests are not responsive to the matters at issue in these comments, nor were they submitted as a reconsideration request.

---

<sup>76</sup> We note that DirecTV agrees with NCTA on this point. DirecTV Comments at 12.

<sup>77</sup> Matsushita Comments at 1-2. This issue is being addressed in a separate proceeding in this docket. *See* NCTA Comments in Docket 97-80 at 10-14 (filed Feb. 19, 2004), responding to Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 7924, 7926 (2003)

<sup>78</sup> DirecTV Comments at 8-10.

<sup>79</sup> NCTA Opposition to Petitions for Reconsideration, at 2-3 (filed March 10, 2004); BellSouth Comments and Opposition at 4 (filed Feb. 25, 2004)

<sup>80</sup> Microsoft Comments at 14-16.

<sup>81</sup> NCTA Opposition to Petitions for Reconsideration and Notice of Joint Proposal for Improved Testing Rules, Docket CS 97-80 (filed March 10, 2004) at Exhibit A.

## CONCLUSION

For the reasons stated above and in NCTA's initial comments, 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

March 15, 2004

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

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

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	<b>NCTA/CableLabs 2004</b>	<b>Microsoft/HP 2003</b>	<b>Microsoft/HP/Dell/Apple 2004</b>	<b>Intel 2004</b>	<b>MPAA</b>	<b>DTLA (Broadcast Flag)</b>
<b>Statement of Position</b>	Comments, February 13, 2004 in CS 97-80	Paula H. Boyd, Microsoft Corporation, and David Isaacs, Hewlett-Packard Corp., to Marlene Dortch, Secretary, FCC (Aug. 8, 2003) 97-80	Comments, February 13, 2004, corrected February 26, 2004 in CS 97-80	Comments, February 13, 2004 in CS 97-80	Comments, February 13, 2004 in CS 97-80 Section x.21(c)(1)(A) - (D) of Appendix A and Part I Comments, February 13, 2004, in MB 02-230. “These criteria would be adjusted to the particular context of DFAST Controlled Content, including the use of a private arbitrator to review initial determinations, the participation of appropriate MVPDs, and the need for numerical copy control functionality and management of copy control information.”	Comments, February 13, 2004 in CS 97-80  Generally supports MPAA proposal as it stood in December, 2002.
<b>Process</b>	May also be approved by 4 studios.	Superseded.	CableLabs as interim, eventually self-certification under new Part 76 rules. Seeks elimination of test suite.	Content Protection approved for one form should be approved for all. Self-certification.	CableLabs, if content owners have a role.	Not addressed.
<b>Video Transport</b>	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?	Not addressed.	Not addressed.	Not addressed.	Not addressed.	Not addressed.
<b>Security Interfaces</b>	How is the security used on the video transport and how is the transport associated with content protection profiles (or encoding rules) and the	Strength of Security. DES, 3-DES, AES should be used. Robust against common circumvention. Simplicity of Security	A content protection method must protect Controlled Content, in conformance with the applicable Compliance Rules, when such content is transmitted among or	A content protection method must protect Controlled Content, in conformance with the applicable compliance	Benchmarked to 5C.	Must specify minimum level of protection, but be flexible enough to allow for innovation.

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	<b>NCTA/CableLabs 2004</b>	<b>Microsoft/HP 2003</b>	<b>Microsoft/HP/Dell/Apple 2004</b>	<b>Intel 2004</b>	<b>MPAA</b>	<b>DTLA (Broadcast Flag)</b>
	<p>methods for authenticating and protecting the content protection profiles?</p> <p>What are the key generation, key protection and key exchange methods used?</p> <p>Are there obvious areas where content is in the clear?</p>	<p>System. Implementing the encryption algorithm in hardware should use &lt;10% of digital logic; in software, should use &lt;3% of processing power used to produce baseband video signal.</p> <p>Rights Expression Language should be flexible and interoperable, like XrML, and defined in industry forum like MPEG-21, Part 5. Authentication. Must be possible to implement in hardware, software, or some combination.</p> <p>For “consistent consumer experience,” minimize consumer confusion about what can be copied from what platforms.</p> <p>Interoperability. Content Protection should be able to communicate with a different Content Protection scheme.</p>	<p>recorded by a variety of consumer devices, including but not limited to single and multi-function devices such as TVs, set-top boxes, game consoles and personal video recorders as well as general purpose devices such as PCs. A content protection method may be implemented in software or hardware or in any combination of the two. In conformance with the applicable Robustness Rules, defeating the content protection method should be beyond the capability of the ordinary user using commonly available tools.</p> <p>The authentication method must ensure that Controlled Content is output to or accessible by another device (including software) only if that device is compliant. This may be accomplished using implicit authentication, such as use of encryption keys that are known only by compliant devices, or using explicit authentication, such as confirming the target device’s ability to protect the Controlled Content consistent with the functional criteria prior to outputting the Controlled Content to the device. The content protection method must securely manage the communication and distribution of any cryptographic</p>	<p>rules, when such content is transmitted to or recorded by one or more consumer devices, including but not limited to single and multi-function devices such as TVs, set-top boxes, game consoles and personal video recorders as well as general purpose devices such as PCs. A content protection method may be implemented in software or hardware or in any combination of the two.</p> <p>The content protection method must provide reasonable constraints to impede the unauthorized use or redistribution (i.e., use or distribution that is inconsistent with the specified usage rights) of Controlled Content delivered over digital cable systems.</p> <p>Interoperability. Content Protection <b>must</b> be able to communicate with a different Content Protection scheme.</p>		<p>This also means that there should be some “reasonableness” standard, rather than warranty that Content Protection will “prevent” unauthorized use.</p> <p>Encryption and key generation is only one method.</p> <p>The encryption algorithm need not be public standard algorithm. Effective proprietary methods must be 56 bit.</p> <p>It is not necessary to specify XrML. Rights generally need not be part of Flag. It should not be necessary that every Content Protection technology be implemented in software or hardware or both. That should be a marketplace choice.</p> <p>It is not necessary that consumer confusion be a selection criteria. Leave it to marketplace.</p> <p>Interoperability is desirable, but not required.</p>

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	NCTA/CableLabs 2004	Microsoft/HP 2003	Microsoft/HP/Dell/Apple 2004	Intel 2004	MPAA	DTLA (Broadcast Flag)
			keys or methods necessary for decrypting the Controlled Content, using specific means to restrict such communication and distribution. Interoperability. Content Protection <b>must</b> be able to communicate with a different Content Protection scheme.			
<b>Security Processing</b>	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?	Robust against common circumvention.	See Robustness.	Not addressed.	Benchmarked to 5C.	Not addressed.
<b>Points of Attack and System Weaknesses</b>	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?	Robust against common circumvention.	All cryptographic algorithms, cryptosystems, keys and secrets shall be of sufficient strength to render breach or compromise of content beyond the capability of an ordinary user using commonly available tools, while meeting applicable export control laws. The encryption algorithm should, in accordance with common and well-regarded security practices, be published and subject to peer review. The algorithm must be such that detailed knowledge of a given implementation of the algorithm shall not, in and of itself, be sufficient to enable the production of circumvention	All cryptographic algorithms, cryptosystems, keys and secrets, or their equivalents, should be of sufficient strength to meet the designated standard of robustness. The applicable robustness rules should require appropriate robust protection of compressed video Controlled Content traversing a user accessible bus in digital form (User	Notes that MS-HP sets robustness level too low, does not define substantive levels of protection in authentication. It would allow encrypted P2P as approved Content Protection.  Benchmarked to 5C.	Controlled Content should not be available on a user accessible bus.

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	NCTA/CableLabs 2004	Microsoft/HP 2003	Microsoft/HP/Dell/Apple 2004	Intel 2004	MPAA	DTLA (Broadcast Flag)
			<p>devices.</p> <p>The Robustness Rules should require appropriate robust protection of content traversing a user accessible bus (<b>excluding without limitation</b> graphics buses, memory buses, CPU buses and other buses that are part of the device’s internal architecture).</p> <p>“PC owners should not have to sacrifice (or lose some of the efficiency of) those functions merely because their PC is capable of receiving content over cable, nor should technologies developed for PCs be excluded from use in digital cable devices solely because the PCs perform additional functions.”</p>	<p>accessible bus means a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard interface, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access.</p> <p>A user accessible bus does not include memory buses, CPU buses or similar portions of the device’s internal architecture that do not permit access to content in a form usable by end users).</p>		
<b>New Algorithms</b>	<p>What is the relative strength of the algorithm?</p> <p>What is the relative strength of authentication with respect to other technologies?</p>	<p>Resistance to obsolescence. Devices that implement encryption algorithm should not hasten obsolescence.</p>	Not addressed.	Not addressed.	Benchmarked to 5C.	Not addressed.
<b>Effectiveness of proposed technology</b>	Does the proposed technology adequately protect content?	Robust against common circumvention.	The content protection method must prevent the unauthorized use or redistribution (i.e., use or distribution that is inconsistent with the specified usage rights) of Controlled Content delivered over digital cable systems.	“There simply is no one size fits all formulation.”	<p>Benchmarked to 5C.</p> <p>The technology is at least as effective at protecting Unscreened Content and Marked Content against unauthorized redistribution (including unauthorized</p>	See Security Interfaces.

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	<b>NCTA/CableLabs 2004</b>	<b>Microsoft/HP 2003</b>	<b>Microsoft/HP/Dell/Apple 2004</b>	<b>Intel 2004</b>	<b>MPAA</b>	<b>DTLA (Broadcast Flag)</b>
					Internet redistribution) as is any one of the technologies then listed on Table A	
<b>Revocation and Renewability of keys</b>	Does the product provide a system key revocation solution? Does the product provide a system key renewability solution?	Upgradeability Renewability  Ability to revoke device or rights to particular content.	Upgradeability Renewability  Ability to revoke device or rights to particular content. The revocation process must be governed by appropriate rules, procedures, and safeguards.	Upgradeability Renewability  Ability to revoke device reception of Controlled Content.	We expect Table A interfaces to have revocation and renewability capabilities.	Requiring renewability and upgradability tilts against CE products in favor of PC products.
<b>DFAST/JTS Consistency</b>	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?	Non-interference with device performance. A device implementing the Content Protection should not behave in noticeable different manner than device not implementing the Content Protection.  Not addressed.	Not addressed.	Not addressed.	Not addressed.	Not addressed.
<b>Licensing Terms</b>	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	Not addressed.	Disclosure of IPR. RAND licensing. Only "reasonable" nonassert or grantbacks. reasonable limits on third party enforcement Process for protecting sensitive	"The Commission should not, however, interfere with the private right to contract by dictating the terms and conditions of private license agreements, or	Output must either impose no obligation or be capable of being remotely turned off.  A determination of whether a technology is "at least as effective" requires	Content owners should have right to participate in change management process to prevent material adverse changes to protection technology.

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	<b>NCTA/CableLabs 2004</b>	<b>Microsoft/HP 2003</b>	<b>Microsoft/HP/Dell/Apple 2004</b>	<b>Intel 2004</b>	<b>MPAA</b>	<b>DTLA (Broadcast Flag)</b>
	<p>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.</p> <p>What license fees are required annually and on each device?            How do the Robustness rules fit with other licensing requirements?</p>		<p>confidential information from disclosure to or misuse by licensors, other licensees or third parties.            Manufacturer right to participate in any change process in the technology.</p>	<p>otherwise even require the licensing of any proprietary technology. Those decisions should all be left to private parties in the market place.”</p>	<p>consideration of the effectiveness of both the technology and any applicable license terms relating to security (i.e., output and recording controls), enforcement and Change Management.</p>	<p>Otherwise, Commission should not involve itself in license terms.</p>
<b>Burden on Cable Network</b>	<p>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.)</p> <p>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</p>	<p>Not addressed. Assumes that renewability may require action at headend.</p>	<p>Not addressed. Focus is exclusively on manufacturer. “These functional criteria are clear enough to allow manufacturers to develop and submit technologies for approval and broad enough to encompass emerging and innovative technologies.”</p>	<p>Not addressed.</p>	<p>Not addressed.</p>	<p>Not addressed.</p>

**Exhibit A**  
**NCTA/CableLabs Comparison of Output Review Proposals**  
**CS Docket 97-80 – March 15, 2004**

	<b>NCTA/CableLabs 2004</b>	<b>Microsoft/HP 2003</b>	<b>Microsoft/HP/Dell/Apple 2004</b>	<b>Intel 2004</b>	<b>MPAA</b>	<b>DTLA (Broadcast Flag)</b>
	the MOU.					
<b>Evaluation Process</b>	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.	Not addressed.	CableLabs as interim, eventually self-certification under new Part 76 rules.	See Process.	Not addressed for UDCP.	Not addressed.
<b>Timetable</b>	A decision will be made within 180 days of receipt of a complete submission.	Not addressed.	Not addressed.	Not addressed.	Not addressed for UDCP. Sets out timetables for flag from public notice, allowing for objection and resolution, effectively within 180 days.	Not addressed.
<b>Appeal</b>	To FCC by any interested party.	Not addressed.	Not addressed.	Not addressed.	Arbitration.	Not addressed.
<b>Relation to Broadcast Flag</b>	Approval for UDCP is approval for broadcast flag, but not vice versa	Not addressed.	UDCP and Flag approvals are independent.	Market acceptance may be part of objective criteria.	Written application. Show usage in the marketplace. A technology may be added to Table A by meeting any one of the following criteria: (1) 3 Major Studios and/or Major Television Broadcast Groups (of which at least 2 must be Major Studios) use or approve the technology; (2) 10 Major Device Manufacturers (including software vendors) have licensed the technology and 2 Major Studios use or approve the technology. (3) meet criteria below.	Approval for UDCP is approval for broadcast flag, but not vice versa