

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

In re

Digital Broadcast Content Protection

MB Docket No. 02-230

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

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

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.

**I. Content Protection and Recording Technology Approval Process**

In both this proceeding and in the proceeding implementing digital transmission and content protection technologies for Unidirectional Digital Cable Products (“UDCPs”),<sup>2</sup> the Commission has sought comment on the appropriate means for reviewing authorized outputs and

---

<sup>1</sup> The Report and Order and Further Notice of Proposed Rulemaking, FCC 03-273, 2003 WL 22494589, was released on Nov. 4, 2003. The Media Bureau extended the comment date for the Further Notice to February 13, 2004 and the Reply Comment date to March 15, 2004. *Order*, DA 03-4085 (Dec. 23, 2003)

<sup>2</sup> *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices*, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 03-225, 2003 WL 22309173 (October 9, 2003) (“*Plug & Play Proceeding*”).

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. *FNPRM* ¶¶61, 62, and 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 the questions raise similar, if not identical issues, that does not mean identical output review mechanisms should be applied in both contexts. As described in NCTA's February 13, 2004 Comments in the *Plug & Play Proceeding*, output and security review of UDCP connectors is part of a transition from a highly secure and proprietary conditional access control system covering the entire distribution path from headend to set-top box to television, to a new regime where retail digital television sets ("DTVs") and other UDCPs have set-top and decryption functionality built inside. If new outputs or new security techniques for UDCPs do not honor the security rules protected by algorithms, security certificates, and key exchanges, a new "digital hole" will be opened that will defeat conditional access, copy control, image constraint, and the very tools cable operators use to protect content and conduct their entire core business. By contrast, content protection for free digital over-the-air broadcast programming is a new adjunct to the broadcast business, and is being implemented in an environment in which the underlying "secured" product is freely available unencrypted for reception and copying by millions of embedded insecure legacy devices.

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." *FNPRM* ¶ 46. Likewise, there is a different level of review appropriate for

outputs and security technologies for UDCPs and for outputs and security technologies for the broadcast flag system.

In comments filed today in response to the Second Further Notice in the *Plug & Play Proceeding*, NCTA describes the dual review mechanisms available for adding outputs or security technologies for UDCPs. Because both of these approaches provide for rigorous review, any output or security technology that is approved for UDCPs under the applicable criteria in the UDCP rules 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 of robustness applied to the broadcast flag is automatically appropriate for the high-value, early release content secured by UDCP 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 should be automatically approved for broadcast flag purposes. However, while a party seeking approval under the UDCP Compliance Rules of an output or security technology that is approved for broadcast flag purposes should note that approval in its submission, that should not in and of itself qualify the output or technology for inclusion under the Compliance Rules until it is reviewed as required for all new technologies under those rules.

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 they have the right to appeal any CableLabs determination to the FCC for review—practically assuring them 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 have revealed a reluctance to place sole control of the “Table A” process with MPAA.<sup>3</sup> On the other hand, there is a benefit to allowing private industry to adopt outputs and security technologies without requiring every innovation to be approved by the government in advance.

We suggest that two paths be provided for adding outputs or security technologies for broadcast flag purposes and evaluating revocation processes incident to each technology. In the first path, objective criteria (similar to those used by CableLabs for UDCPs<sup>4</sup>) 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 at the outset, eliminating concerns that a single entity could block approval of a new output or security technology.

## **II. Encrypting the Digital Basic Tier**

In adopting the FNPRM in this proceeding, the Commission took note of NCTA’s suggestion that by permitting cable operators the option of encrypting the digital basic tier, operators could pass a virtual broadcast flag that would enhance the offering of future home networking services in a secure environment. See *FNPRM* ¶ 59. The rules as adopted provide that where MVPDs encrypt the retransmission of broadcast signals, they may convey the intent of the flag through the MVPD’s system to protect the content as if the flag were present.

---

<sup>3</sup> See Comments of Philips Electronics North America Corporation, at 25-28 (December 6, 2002); Letter from CFA, Consumers Union, Public Knowledge and AAI to Chairman Powell, at 2-3 (October 21, 2003).

<sup>4</sup> See Comments of the National Cable & Telecommunications Association, CS Docket No. 97-80, at 14-16 (February 13, 2004).

To effectuate this option, however, may require a change in the Commission's rules. Section 76.630(a) of the current rules provides that "cable system operators shall not scramble or otherwise encrypt signals carried on the basic service tier." The Commission may need to amend -- or provide a blanket waiver of -- Section 76.630(a) to permit (but not require) scrambling of digital broadcasts by cable operators if incident to implementation of the broadcast flag. As we have stated in an earlier stage of this proceeding, permitting encryption of the digital basic tier will allow optimal use of existing secure transport technologies and facilitate home networking while protecting the content from indiscriminate redistribution.<sup>5</sup> We urge the Commission to amend its rules to permit such encryption.

### **III. Conclusion**

For the reasons stated above, NCTA requests that the Commission permit the use of UDCP-approved technologies in the broadcast flag context, but not allow broadcast flag technologies to be automatically implemented in the more secure environment required for UDCPs without the further review applied to UDCP products. Further, the Commission should amend its rules to allow operators the option of encrypting the digital basic tier so that consumers

---

<sup>5</sup> See NCTA Reply Comments at 4-7 (Feb. 20, 2003).

may utilize the free programming they receive but still have that programming be subject to the content protections carried with the flag.

Respectfully submitted,

**/s/ Daniel L. Brenner**

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

Andy Scott, Senior Director, Engineering

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

National Cable & Telecommunications  
Association  
1724 Massachusetts Avenue, N.W.  
Washington, D.C. 20036-1903  
202-775-3664

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](mailto:pglist@crblaw.com)

February 13, 2004