

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

In re Digital Broadcast Content Protection

MB Docket No. 02-230

**THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION'S
OPPOSITION TO PETITIONS FOR RECONSIDERATION**

The National Cable & Telecommunications Association (“NCTA”), pursuant to Section 1.429 of the Commission’s Rules, 47 C.F.R. § 1.429, hereby opposes the Petition for Reconsideration and Clarification submitted in this proceeding by the Motion Picture Association of America, Inc. (“MPAA *Flag Recon*”), the Petition for Reconsideration filed by Genesis Microchip, Inc. (“Genesis”), and the joint petition filed by the National Music Publishers’ Association, the American Society of Composers, Authors and Publishers, the Songwriters Guild of America and Broadcast Music, Inc., (“Music Publishers”). All three petitions seek reconsideration of parts of the Commission’s *Report and Order*¹ in the above-captioned proceeding.

I. Robustness Rules Governing Demodulator Products – MPAA

In formulating the robustness rules for determining how digital televisions (DTVs) and related devices would respond and give effect to the ATSC broadcast flag, the Commission rejected an “expert” level of robustness proposed by MPAA and the 5C companies. *Flag R&O*, ¶ 46. Instead, the Commission found that a more generalized robustness standard set at an

¹ *In re Digital Broadcast Content Protection*, MB Docket No. 02-230, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 03-273, 2003 WL 22494589 (rel. Nov. 4, 2003), 68 Fed. Reg. 67599 (Dec. 3, 2003) (“*Flag R&O*”). Petitions for reconsideration were filed on January 2, 2004. The Media Bureau extended the date to file oppositions to the petitions for reconsideration up to and including March 10, 2004. *Order*, DA 04-260 (Feb. 3, 2004)

“ordinary user” level would be more appropriate as it would afford CE, IT and PC manufacturers with flexibility in determining how to effectuate compliance and ensure security of content. *Id.* More importantly, “because DTV broadcast material will be delivered over-the-air in the clear, it would not be reasonable to require as high a robustness level as provided for DVDs, for example, which are delivered in a scrambled protected form.”² The Commission also said it would entertain complaints if a product or manufacturer does not meet this baseline standard. *Flag R&O*, ¶ 46.

In its Petition, MPAA repeats its earlier concerns and urges the Commission to reconsider and ratchet up the level of robustness to thwart the “skilled user.” MPAA argues that its original proposal was almost the same as the robustness standards applied to encrypted content systems (*e.g.*, DTCP) so it should create no additional burdens on manufacturers or others implementing the broadcast flag. MPAA also argues that hacks that are created by professionals, translated by others into scripts and instructions and then disseminated over the Internet in a form ready to use by common users, are not “ordinary user” hacks and therefore would not be stopped if the standard adopted by the FCC is retained.³ MPAA asks that the FCC adopt its original proposal with no change. MPAA’s analysis is flawed and its reconsideration request should be denied.

The Commission’s decision with respect to the appropriate level of robustness for devices implementing the broadcast flag is supported by an instructive comparison to rules adopted for Unidirectional Digital Cable Products (“UDCPs”).⁴ As described in NCTA’s Further Comments in the *Plug & Play* proceeding, output and security review of UDCP connectors is part of a

² IT Coalition Comments at 21, note 64.

³ MPAA Petition at 17-19.

⁴ Implementation of Section 304 of the telecommunications Act of 1996, Commercial Availability of Navigation devices and Compatibility Between Cable Systems and Consumer Electronics Equipment, CS Docket 97-80 and PP Docket No. 00-67, *Second Report and Order and Second Further Notice of Proposed Rulemaking* (rel. Nov. 4, 2003), 2003 WL 22309173, 68 Fed. Reg. 66728 (Nov. 28, 2003) (“*Plug & Play*”).

transition from highly secure proprietary conditional access to retail digital television sets (“DTVs”) with set-top functionality built inside.⁵ If new outputs or new security techniques for UDCPs do not provide sufficient security assurances including a high level of robustness, a new “digital hole” will be opened. That hole will undo conditional access, copy control, image constraint, and the very tools that enable cable operators to negotiate with program suppliers for high value digital content to provide to their customers, while offering such program suppliers a reasonable assurance that such content will be protected from illegal access.⁶ A significant compromise of reception or copy controls for encrypted, high-value cable programming could lead content providers to refuse delivery of high-value content to cable systems and their customers.

By contrast, the broadcast flag is a new adjunct to the broadcast business and is being implemented in an environment in which the underlying “secured” product is available unencrypted, free, over-the-air and available for reception and copying by millions of existing legacy devices. If there is to be a “hack,” it will most likely occur before demodulation, not after demodulation by a compliant device. The skilled “professional” hacker would only need an off-air antenna to defeat the flag.

We also do not accept the premise that a “hack” widely disseminated and available on the Internet for ready use by ordinary users, as posited by MPAA, would not violate the FCC’s robustness standard.⁷ The robustness rules will still require that the flag be protected so that it cannot be defeated or circumvented merely by an ordinary user using generally-available tools or

⁵ NCTA Comments (*Plug & Play* proceeding) at ii, 19 (filed Feb. 13, 2004.).

⁶ *Id.* at 19.

⁷ MPAA Petition at 7-8.

equipment. The anti-circumvention rules in the DMCA would also apply.⁸ Accordingly, the Commission was correct when it found that an expert level of robustness for the broadcast flag would be “incongruous with the scope of protection offered by an ATSC flag system.” *Flag R&O*, ¶ 46.

NCTA supports the use of the broadcast flag to prevent the unauthorized distribution of broadcast content over the Internet. However, the flag should not become an excuse for the micromanagement of MVPD networks, as it could under the MPAA proposal. Seeking a professional level of robustness when the underlying product is not even secured at the source is merely inviting unnecessary review of the elements of secure networks that have more than adequate business incentives to maintain their security. For decades, cable operators have been maintaining conditional access networks that are secure enough to meet their own needs to protect subscription revenue against theft and to satisfy suppliers of high-value programming in an earlier release window than over-the-air broadcast programming.

NCTA’s concern over possible misuse of the broadcast flag rules is also reflected in our request (on reconsideration) that the Commission not freeze QAM modulation technologies at 256 QAM.⁹ MPAA has informed us of its view that the flag regulations require any new MVPD modulation technique to encrypt the basic broadcast service.¹⁰ Whether or not encryption of broadcast should be an *option* in specific applications, as NCTA believes it should be, it is inappropriate to convert the broadcast flag rules into the controlling vehicle dictating the transport techniques used by MVPDs.

⁸ 17 U.S.C. § 1201.

⁹ NCTA Petition for Reconsideration, filed January 2, 2004 at 2-3.

¹⁰ Indeed, in its comments in response to the Further Notice in this proceeding, MPAA is urging the Commission to *require* that cable operators encrypt the basic tier. Comments of MPAA and Movie Studios, filed Feb. 13, 2004, at 11-13.

The same concern about overreaching is reflected in our request that the Commission clarify that the broadcast flag does not control secure transport around robust home networks where the programming remains under the sole control of a cable operator's "gateway" device.¹¹ Adopting the robustness regime proposed by MPAA would convert the broadcast flag rules into a tool by which MPAA, its member studios, or anyone else passing judgment on robustness or robust connections could control every element of an MVPD's transport and the architecture of a secure home network. That is far beyond the announced and proper purpose of the flag to restrict unauthorized Internet redistribution of free, over-the-air, broadcast programming.

If for any reason the FCC chooses to amend the robustness rules, it should preserve the right of secure transport around robust home networks where the programming remains under the sole control of a cable operator's "gateway" device. It should adopt the same approach as we have recommended for output review: if a device or connection in an MVPD's network is robust enough for approval under the DFAST license for "Plug and Play" products and to satisfy the needs of a truly secure system, no further review or approval of the robustness of such a device or connection should be required for broadcast flag purposes.¹²

II. DVI and the Broadcast Flag – Genesis Microchip

Genesis Microchip raises a series of challenges that reflect its dissatisfaction with the outcome of marketplace dynamics, its misunderstanding of the flag technologies, and a particular challenge to DVI. At bottom, its concerns reflect its losing position in private litigation with Silicon Image over patent issues regarding DVI and HDMI connectors. NCTA addressed those issues in detail in its opposition to the reconsideration petitions in the *Plug and Play* proceeding,

¹¹ NCTA Petition for Reconsideration at 6-10.

¹² NCTA Comments at 19 (Filed Feb. 13, 2004)

including Genesis Microchip's petition there which raises the same issues.¹³ We incorporate by reference herein our response to the Genesis arguments. As we explained there in detail, the FCC is not the appropriate venue to resolve Genesis Microchip's patent litigation problems.

III. Audio Outputs – Music Publishers

A group of music publishing entities also jointly sought reconsideration in this proceeding.¹⁴ This same group filed jointly for reconsideration in the *Plug and Play* proceeding and cited to and relied upon their *Plug and Play* petition in making their request for reconsideration in this proceeding.¹⁵ Accordingly, NCTA incorporates by reference herein its response to the Music Publishers' arguments filed today in that proceeding.¹⁶

¹³ NCTA Opposition to Petitions for Reconsideration and Notice of Joint Proposal for Improved Testing Rules, Docket No. 97-80, at 5-9 (filed Mar. 10, 2004).

¹⁴ Music Publishers' Petition for Reconsideration (filed Dec. 31, 2003)

¹⁵ *Id.* at 3, 4.

¹⁶ NCTA Opposition to Petitions for Reconsideration and Notice of Joint Proposal for Improved Testing Rules, Docket No. 97-80, at 9-14 (filed Mar. 10, 2004)

CONCLUSION

For the foregoing reasons, NCTA urges the Commission to deny the petitions for reconsideration filed by MPAA, Genesis Microchip and Music Publishers.

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 10, 2004

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

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

CERTIFICATE OF SERVICE

I, Judith A. Easterday, do hereby certify that a copy of the foregoing “National Cable & Telecommunications Association’s Opposition to Petitions for Reconsideration” was served by United States First Class Mail, postage prepaid, this 10th day of March 2004 on the following:

Bruce E. Boyden, Esquire
Proskauer Rose LLP
1233 Twentieth Street, N.W.
Suite 800
Washington, D.C. 20036

Carl Hampe, Esquire
Baker & McKenzie
815 Connecticut Avenue, N.W.
Suite 900
Washington, D.C. 20006

Robert J. Ungar, Esquire
Fish & Richardson, P.C.
1425 K Street, N.W.
Suite 1100
Washington, D.C. 20005

/s/ Judith A. Easterday