

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

In re Digital Broadcast Content Protection

MB Docket No. 02-230

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

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

I. Encrypting the Digital Basic Tier

In its initial comments in response to the *FNPRM*, NCTA reiterated its request that the FCC expressly provide cable operators with the option, already exercised by DBS providers, of encrypting the digital basic tier and conveying a virtual broadcast flag.²

Other Comments in response to the *FNPRM* ranged from vehement objections to any encryption *at all* to insistence that any new QAM modulation for basic *must* be encrypted. The objections of the Consumer Electronics Retailers Coalition (“CERC”), the Consumer Electronics Association (“CEA”), and the Home Recording Rights Coalition (“HRRC”) are based on two mistaken premises. First, CERC contends that encrypting basic would “lock out” DBS

¹ The Report and Order and Further Notice of Proposed Rulemaking, FCC 03-273, 18 FCC Rcd 23550, 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)

² NCTA Comments at 4-5 (filed Feb. 13, 2004); *FNPRM*, 18 FCC Rcd at 23577 (¶ 59).

providers' products from home networking.³ HRRC similarly claims that encrypting basic would allow cable operators to seize control of home networking at a home gateway device and confine it within a closed, anti-competitive cable-controlled home network.⁴ Second, CEA claims that encrypted basic would disenfranchise viewers and turn the CableCARD itself into a home gateway device.⁵

As to the first concern regarding the impact of encrypting the basic tier on home networking, the concerns expressed by CEA and HRRC are misplaced. If a cable operator were to encrypt a digital basic tier, any customer could use a CableCARD or set-top box to decrypt the signal(s) once, and then transport the signal(s) around the home without the use of any cable-controlled conditional access.⁶ Mechanically, programming is received and decrypted (for viewing) at the first CableCARD-enabled device or set-top box. There is no requirement that downstream devices inside the home use coaxial cable, DigiCipher, PowerKey, NDS, or any other conditional access tool used on a cable operator's outside plant.

We anticipate that there will be multiple, competing home networks using wired and wireless connections and a variety of content protection techniques (or in this case, flag

³ CERC Comments at 2.

⁴ HRRC Comments at 3.

⁵ CEA Comments at 3.

⁶ CERC argues that encrypting basic would add unnecessary robustness rules to receiving devices. CERC Comments at 2. CERC is mistaken. A DTV without a CableCARD slot but with an 8-VSB tuner would handle broadcast signals in whatever robust manner is required by the broadcast flag rules. If a DTV includes an optional CableCARD slot to become "digital cable ready," then both the broadcast flag robustness rules (applicable because a UDCP must have an 8-VSB tuner) and the DFAST robustness rules—to which CE manufacturers have agreed for UDCPs—would apply. If broadcast signals were encrypted, signals decrypted by the CableCARD for a CableCARD-enabled UDCP would not trigger any new robustness rules, because the UDCP is already subject to them by virtue of including a CableCARD slot to be "digital cable ready." CERC alludes to some new unnamed, undescribed, small ancillary devices that might be intended to receive only basic broadcast signals from cable and no other cable signals. CERC Comments at 2. But if these devices are designed to receive digital broadcast signals, they would need to meet broadcast flag robustness rules in any event. If they are actually so limited and ancillary, they could be attached downstream of an off-air DTV, downstream of a DTV connected to a set-top box, or downstream of a CableCARD-enabled product, and they would not need decryption, would not need a CableCARD slot, and would therefore not need to meet CableCARD robustness rules.

preservation techniques). Nothing in the proposal to allow encryption of the basic tier retards competitiveness—it only provides cable operators with the same options as DBS, whose (encrypted) broadcast services are received on millions of TVs. The concerns of CEA, CERC, and HRRC over home networking are without substance.

As to the concern that encrypting the basic tier would disenfranchise viewers and turn the CableCARD into a home gateway device, that too is misplaced. The rule prohibiting encryption of analog broadcast signals and, by extension, the entire analog basic tier, emerged because there were so many television sets deployed with the ability to receive unencrypted broadcast signals over cable without the use of a set-top box. Given the wide deployment of standard analog tuners, it was deemed to be in the public interest to prohibit the encryption of analog basic tier signals so consumers who purchased analog television sets and VCRs with tuners capable of tuning basic service channels would not be required to acquire a cable set-top box to view those signals because they could view the local broadcast signals “over-the-air” without additional equipment in the absence of cable.⁷ Under those circumstances, if a broadcast signal on a cable operator’s basic tier was encrypted, one could argue (although not very persuasively) that a cable customer had been “disenfranchised” in the sense he would have to acquire a set-top box to view signals over cable that he or she could get free over-the-air.

By contrast, there are relatively few digital television sets with QAM receivers that can tune to cable-delivered *digital* broadcast signals. The vast reservoir of embedded “legacy” TV’s that CERC claims would be locked out by encryption of the basic tier cannot tune to a digital tier without a digital set-top box. And, to the extent those consumers had digital cable ready DTV

⁷ *Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Report and Order, ET Docket 93-7, 9 FCC Rcd 1981, 1990 (¶ 49) (1994) (“*1994 Compatibility Report and Order*”).

sets which did not require a set-top box, it is more likely than not that—as high-end consumers—they would need to obtain a CableCARD for decryption of the premium and other scrambled non-broadcast programming they likely would order. That CableCARD would decrypt encrypted broadcast programming as well. As a result, permitting the option of encryption of digital broadcast signals would have little effect on consumers who wish to view cable’s digital offerings. In any event, they would either require a digital set-top box or likely order a CableCARD.⁸

At the other extreme is MPAA, which has requested that any new QAM modulation for basic *must* be encrypted. We do not believe that the use of the flag should compel encryption in all cases, only that encryption of digital basic should be one permitted tool. As we explained in our initial comments, encryption of the basic tier should be an option because it provides a means for conveying the flag in a manner which makes use of the secure transmission advantages of the cable system and also allows the operator to help prevent theft of the basic tier just as DBS operators do.⁹ But there are sure to be cable operators who would chose techniques other than encryption, due to cost, convenience, or otherwise.

In that regard, *requiring* encryption of the basic tier is another matter. There are multiple ways to address security, especially in smaller markets, and encrypting all tiers is only one. In addition, as we have said elsewhere, a professional hacker would only need an off-air antenna to defeat the flag. It is not appropriate to convert the broadcast flag rules into a tool by which

⁸ CEA also claims that no redistribution or copy protection function is served by encryption. CEA Comments at 3. As MPAA notes, cable operators have an independent right to secure their networks against theft. MPAA Comments at 12. But in this case, encryption also provides a means for conveying the flag in a manner which makes use of the secure transmission advantages of the cable system. The Commission recognized that it may have to revisit its policy towards encryption when developing digital cable standards. *1994 Compatibility Report and Order*, 9 FCC Rcd at 2005 (¶ 144).

⁹ *Id.* at 1991 (¶ 57). DBS encrypts every programming service it provides, including local and distant broadcast signals.

MPAA and its member studios can dictate cable operators' transport technology. Cable operators need the option of selecting other possible tools that may be more suited for particular markets or systems.

NCTA's request that the FCC grant cable operators the *option* of encrypting the digital basic tier and conveying a virtual broadcast flag is a fair, pro-competitive middle ground. The Commission should revise the rules to allow, but not require, encryption of cable's basic tier.¹⁰

II. Content Protection and Recording Technology Approval Process

As described in NCTA's prior Comments, 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.¹¹ 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.

There are also different functional requirements: copy protection is not a required functionality for getting on Table A. CEA, MPAA, the Digital Transmission Licensing

¹⁰ NCTA Comments at 4-5; 47 C.F.R § 76.630(a).

¹¹ *See generally* Comments of NCTA at 2-3 (filed Feb. 13, 2004); Comments of NCTA, submitted in CS Docket No. 97-80, at 19-20 (filed Feb. 13, 2004).

Administrator, LLC (“DTLA”), Microsoft, Philips, Matsushita, Public Knowledge, and others agree that the two regimes should not be unified.¹² In our initial Comments, we suggested that devices which are approved under the more demanding requirements for UDCPs should automatically be approved for broadcast flag. MPAA agrees, assuming appropriate rights in the CableLabs process.¹³ DTLA agrees, noting that this approach eases everyone’s burden, by starting with the more protective regime.¹⁴

We also suggested 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 UDCPs¹⁵) 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. A similar approach is proposed by DTLA.¹⁶ As we explain in detail in our Reply Comments in the related proceedings for UDCPs,¹⁷ this dual track approach provides appropriate paths that permit innovation but do not create the risks incident to pure self-certification.

III. Professional Equipment

In NCTA’s Petition for Reconsideration, we recommended the adoption of a professional equipment exemption which we drafted to account for the needs of MVPDs. Harmonic has

¹² CEA Comments at 4; MPAA Comments at 3; DTLA Comments at 13-14; IT Coalition Comments at 14-15; Philips Comments at 29-30; Matsushita Comments at 1-2; Public Knowledge Comments at 17. *See also* Microsoft Comments (part of IT Industry Comments), submitted in CS Docket No. 97-80, at 7-8, n.10 (filed Feb. 13, 2004).

¹³ MPAA Comments at 2-3.

¹⁴ DTLA Comments at 3.

¹⁵ See Comments of NCTA, CS Docket No. 97-80, at 14-16 (Feb. 13, 2004).

¹⁶ DTLA Comments at 17-18.

¹⁷ NCTA Reply Comments, submitted in CS Docket No. 97-80, at 8-9 (filed March 15, 2004).

endorsed and expanded this proposal to cover other legitimate professional uses.¹⁸ We support Harmonic’s suggestion.

IV. Personal Digital Network Environments (“PDNEs”)

The Commission’s question about PDNEs has provoked a considerable difference of opinion over what is or will be permitted redistribution of programming outside the home. MPAA is willing to extend use to a “tightly defined geographic area around a Covered Product.”¹⁹ Philips asks for “tailored, point to point” Internet redistribution to office, mobile devices, and second homes.²⁰ CEA takes the next step, asking for a “close personal affinity group” including family and friends, mobile use, and coworkers.²¹ HRRC takes the final plunge, asking that “fair use” set the standard and redistribution to friends and family be broadly defined to limit incentives to hack the flag—apparently by rendering it pointless.²²

We respectfully submit that the Commission should not attempt to answer the PDNE question. The question has already led to requests that the Commission create a “safeharbor” of fair use across the Internet. As others have observed, it is terribly premature to attempt to define that scope.²³ It involves highly contentious issues of copyright law, as Joint Sports makes clear.²⁴ It conflates *ex ante* tools—technological measures that prevent certain distribution—with *ex post* rules—the right of content owners to enforce copyright laws against infringers, from which Internet redistributors are seeking a safe harbor. Nor do the tools even exist for distinguishing what is “tailored” redistribution and who are family, friends, acquaintances or

¹⁸ Harmonic Comments at Parts III and IV.

¹⁹ MPAA Comments at 8.

²⁰ Philips Comments at 30.

²¹ CEA Comments at 6.

²² HRRC Comments at 4.

²³ See Time Warner Comments at 12; MPAA Comments at 8; DTLA Comments at 16-17, IT Coalition Comments at 6-8; Verizon Comments at 3-6; Public Knowledge Comments at 11-13.

²⁴ Joint Sports Comments at 6.

coworkers. The scope of redistribution outside the home needs to evolve through marketplace negotiations and the development of refined tools, the details of which cannot be fairly anticipated by the Commission.

CONCLUSION

For the reasons stated above, NCTA requests that the Commission (1) afford cable operators the option to encrypt the basic tier; (2) maintain separate UDCP and broadcast flag approval processes, but treat outputs and content protection technologies which are approved under the more demanding requirements for UDCPs as automatically approved for broadcast flag; (3) adopt the professional equipment exemption proposed by NCTA and Harmonic; (4) and not attempt to define acceptable contours for redistribution of content over PDNEs at this time.

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
pghost@crblaw.com

March 15, 2004