

PROSKAUER ROSE LLP

DOCKET FILE COPY ORIGINAL

1233 Twentieth Street NW
Suite 800
Washington, DC 20036-2396
Telephone 202.416.6800
Fax 202.416.6899

NEW YORK
LOS ANGELES
BOCA RATON
NEWARK
PARIS

Jon A. Baumgarten
Member of the Firm

Direct Dial 202.416.6810
jabaumgarten@proskauer.com

May 24, 2000

Ms. Magalie Roman Salas
Office of the Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

RECEIVED
MAY 24 2000
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

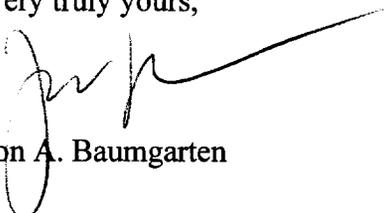
Re: Compatibility Between Cable Systems and Consumer Electronics Equipment
-- PP Docket No. 00-67

Dear Ms. Salas:

Please find enclosed comments by the Motion Picture Association of America, Inc. in the above-referenced proceeding.

Any questions regarding this submission should be directed to the undersigned.

Very truly yours,


Jon A. Baumgarten

No. of Copies rec'd 0+9
List ABCDE

2000

RECEIVED

MAY 24 2000

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

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

<p>In the Matter of</p> <p>Compatibility Between Cable Systems And Consumer Electronics Equipment</p>	<p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p>	<p>Comments of Motion Picture Association of American to NPRM</p> <p>PP Docket No. 00-67</p>
---	--	--

I. Preliminary Statement

The Motion Picture Association of America, Inc. (MPAA) submits these comments in response to the Commission's Notice of Proposed Rulemaking "In the Matter of Compatibility Between Cable Systems and Consumer Electronics Equipment," PP Docket No. 00-67. As a preliminary matter, we note that the issues leading to this rulemaking are fundamentally related to influence over consumer electronics equipment and navigation choices. Content and content protection should not be "put into play" by participants in that debate. Our purpose is to insure that there is valuable content that consumers can access, regardless of whose or what navigation system they may use.

That purpose is particularly endangered today. A review of major newspaper articles and specialized publications over just the last few weeks dramatically shows the growing numbers of software, services, and devices capable of facilitating, and in some cases designed to promote, the illegal copying and distribution of content providers' valuable content.¹ For example:

- Broadband capacity and corresponding modems and related connections are regularly and increasingly available to consumer markets, enhancing the speed and capacity of motion picture downloading, transmission, and retransmission within and across the Internet, intranets, and other multiple user arrangements (including those described below).

¹See, e.g., "E-Power to the People; New Software Bypasses Internet Service Providers," Washington Post, May 18, 2000 at 1. "Cyberspace Programmers Confront Copyright Laws," New York Times, May 10, 2000 at 1; "Is Copyright Dead," PC Magazine, June 6, 2000 at 85. Bob Sullivan, Movie Pirates Hitting Prime Time (visited 5/24/00) <<http://www.msnbc.com/news/402970.asp>>

- New digital storage media suitable for retention and downloading of full-length motion pictures are rapidly emerging for consumer use. These include a number of formats of recordable DVD, various models of dedicated hard drive recorders, both free-standing and integrated with receivers ("personal video recorders"), digital videotape in consumer configurations, "swappable" hard drives, and ever-expanding removable computer storage discs, cartridges and other devices.
- New video tools such as "DivX" have been devised that enable compression of motion picture files for ready consumer storage and transmission of full length motion pictures in digital form.
- New software, sites, and arrangements for both relatively decentralized and wholly decentralized "user-to-user" (or "peer-to-peer") Internet distribution are daily emerging that are targeted at the unauthorized reproduction and distribution of complete motion pictures among great numbers of users. "Scournet," "Freenet," and "Gnutella" are recent examples. These services are frequently designed with techniques that hide or obfuscate the identity of participating users in order to forestall copyright enforcement. In a number of cases the developers and/or users of these services do not hesitate to proclaim their utility for ignoring intellectual property rights.²
- A determined hacking community stands ready to devise, employ and disseminate these capabilities.

Some of these developments are neutral in their design or purpose; others are not. But, both independently and together, they mark an environment that will enable the simple, inexpensive, and unauthorized widespread replication, duplication, transmission and redistribution of motion pictures, television programs and other copyrighted works that are not sufficiently technologically protected.

²The Commission is aware of the MP3 compression technology that has facilitated massive unauthorized copying and distribution of unprotected musical recordings on the Internet. The developments noted above are able, and in some cases designed, to produce this result for motion pictures. "Wrapster," for example, is software designed to cloak movie files to look like MP3 music files in order to facilitate unauthorized copying and distribution by "Napster" and other utilities and services that were initially developed for unauthorized copying of music files. "Scournet" may be an example (in some ways similar to the music-oriented "Napster") of a relatively decentralized user-to-user system because a common facility is involved in at least searching, identifying and facilitating retrieval, reproduction and distribution, while immediate storage and/or transmission may be spread out among many users. "Freenet" and "Gnutella" are allegedly wholly decentralized in that searching, retrieval, and distribution reportedly do not share a common hub.

II. Summary

The FCC and MPAA share a common goal of encouraging and facilitating deployment of digital television services. Compelling content and viewer options are essential to this goal.³ Technically sophisticated hardware will not alone ensure the success of digital television; content and viewing options are critical ingredients.

Digital technology offers the promise of enhanced content and new viewing options that can accelerate the adoption of digital television in this country. But digital technology also poses extraordinary risks to the viability and fulfillment of the promise of digital television. This is not merely because "with a digital source, high quality copies can be made and further reproduced with virtually no degradation in quality" (FCC NPRM text following fn. 28). Although that statement is true, the digital phenomenon of the "endless perfect master" is only the tip of a very large iceberg of risk described in Part I above.

Worldwide theatrical and post-theatrical markets are significantly threatened by the developments described in Part I. Theatrical markets are endangered, for example, by the unprecedented potential for digital reproduction and transmission from purloined exhibition copies, and from post-theatrical release copies and television exhibitions in the United States while a motion picture is still in theaters abroad. Post-theatrical markets are particularly at risk. These markets include broadcast, pay, pay-per-view, basic cable, satellite, video (tape), DVD, video and subscription-on-demand, and future examples such as portable playback and Internet delivery. Viable post-theatrical markets are essential to the motion picture industry since theatrical receipts alone generally account for only about 20% of total film revenues and are rarely sufficient to recoup investment in production and distribution. Content protection is essential to the viability of those markets and to similar markets for television programs, and to the emergence of even newer options for viewer enjoyment.

Adequate, effective content protection is therefore critical to content owners, to their willingness to expose their content to the digital marketplace and develop innovations in services, and hence to the rapid deployment and adoption of digital television and to achieving its promise. For the reasons given in Part III B below, Circuit City's suggestion that content protection across a POD-host interface is forbidden by the Commission is technologically unsound and substantively unsupportable.

³Each MPAA member company will, of course, make independent business decisions concerning these matters. The purpose of our comments is to assure a secure framework in which such individual decisions can be made and that is conducive to decisions that will promote the transition to digital television.

Consumers deserve the best that content providers can responsibly give them in terms of programming content and viewing options. Exposing content to potential massive misuse is not responsible business behavior. Consumers also need a clear understanding of the capabilities of purchased equipment. If certain equipment will not receive all content because such equipment does not accommodate the content protection needs and responsibilities of content owners, then consumers must be made aware of the limited capabilities of such equipment so that they are not confused.

The Commission obviously cannot regulate what individual content providers may choose to put at risk, what risk, if any, is acceptable, or what price, terms or conditions, a content provider should pay, or assent to, for content protection. For this (and other) reason(s), the Commission cannot and should not seek to regulate the terms of content protection technology licensing agreements. This should not, however, hamper the deployment of properly labeled hardware devices that manufacturers may choose to make available in any configuration.

In order to enable content protection of non-premium digital services, scrambling or encryption of such programming must be permitted across the POD interface. As discussed below, 47 C.F.R. 76.30 does not and cannot apply to digital content.

III. Questions⁴

A. Labeling and Related Issues

The Commission asks what "digital services consumers will be able to access with a television receiver that meets the standards specified in the CEA-NCTA agreement [for direct connection of televisions to cable services and navigation support] and no additional operator-supplied equipment." (Paragraph preceding fn. 42.) From the content providers' perspective, this remains within the discretion of individual providers. However, for the reasons given earlier, it is clear that an absence of adequate and effective content protection must result in an environment where individual content owners will be substantially impeded in providing content and viewing options.

The foregoing conclusions underlie our answers to the Commission's questions on consumer labeling. Any designation that states or implies that receiving apparatus is "cable-ready" should be restricted to receivers that provide effective content protection. Specifically, "cable-ready" receivers must (a) incorporate a POD security module that (b) itself employs encryption and authentication for protection of content delivered across the POD-host interface and (c) is subject

⁴This section seeks to answer specific questions pertaining to particular matters raised by the Commission. There are other technologies and methods that are vitally important to content protection, such as recognition of extended copy control information (ECCI) and watermarks, that are not addressed here.

to decryption/authentication licensing that imposes content protection obligations on the host. Moreover, the Commission should consider adoption of a regulation that if a receiving device is not labeled as "cable-ready" for any reason (including failure of any of the above conditions), there must be meaningful public disclosure to consumers of what services will not be received. We would be pleased to work with the Commission to develop forms of such disclosure.

It is only when the three conditions described immediately above are met that any receiving apparatus may reasonably be expected to deliver the broad array of content and viewing options that should come to characterize digital television. The absence of any one or more of these conditions will subject the content to misdirection (e.g., to the Internet) and other misuse (e.g., interception, copying and/or endless replication); will enable uncontrolled retransmission and copying by devices that can deceive or "spoof" the POD into delivering content for such misuse; and will eliminate content protection within and from outputs of even benign host devices once they are available at retail and divorced from direct influence by cable operators and indirect (sublicense) contractual influence by content owners. The use of "cable-ready" or any similar designation to designate equipment that does not meet each of these conditions would be uninformative, deceptive, or at best confusing to consumers, resulting in erroneous purchasing decisions. Receiving devices that fail to meet any of these three conditions cannot reasonably be considered "cable-ready" since they will most likely not receive important categories of programming. The Commission's concern that "digital television receivers be able to display the digital broadcast signals (and other programming) that cable systems offer and that consumers have a clear understanding of the capabilities of the digital television receivers that they purchase [NPRM at 10 (emphasis added)]" will be defeated. (We do not believe that there is an easily understood one or set of "alternative designation(s)" that will resolve this issue in a different manner. NPRM fn. 34 and ¶ 18.)

Until now, consumers have been generally choosing among television sets that were technologically capable of receiving all programming. Because this may no longer be the case, the Commission's concern for "consumer understanding" will also be served by the supplemental regulation we have proposed for receivers that are not labeled as "cable-ready." Consumer confusion in the digital television marketplace can only delay and impair adoption of such technology.

The above conclusions also provide our answers to the Commission's questions on the relationship between the availability of 1394 connectors and labeling of receivers as "cable-ready." More specifically:

- A fully integrated television receiver that connects directly to a cable system without the intervention of a set top box should not require a 1394 or other particular connection at its inputs to be considered "cable ready"; it must, however, meet each of the three conditions described in the third paragraph above with respect to POD and host in order to be "cable-ready." (In this context, the receiver will be the "host" and will incorporate a separate "POD". Because of the

conditions described above, the outputs and operation of the integrated receiver will protect the content under the terms of the technology license.)

- A television receiver that is not fully integrated and connects to a cable system through a set top box, and the set top box itself, must provide content-protecting connections in order to be considered "cable ready." If it does not, content providers cannot at this time have confidence that a framework will exist to provide adequate and effective content protection. At this time, 1394 connections with DTCP to other digital devices, and DVI connections with HDCP to display devices, are two available digital interfaces that meet these conditions.

B. Licensing of Content Protection Technologies

As described earlier, it is essential to content providers' needs for content protection that their content be encrypted across the POD-host interface. Encryption cannot reasonably stop upon receipt at the POD - that may serve cable operators' security of their paying-subscriber base, but does nothing to protect content from misdirection and misuse in, from, and by host devices. Without protection across the POD interface, content is completely vulnerable to unauthorized transmission and copying, including by unintended hosts disguised to the POD as innocent receiving devices.

It is equally essential to an adequate and effective content protection framework that there be meaningful content protection terms and conditions imposed on the internal operation (e.g., integrated digital recorders) and outputs (e.g., to the Internet and to other receiving, copying and retransmitting devices) of host devices. Pursuant to the Commission's rules governing separation of system security and navigation and providing for retail availability of all host devices, those terms and conditions cannot otherwise be effectively negotiated or imposed on the hosts either directly or through sublicensing by cable operators. CableLabs' licensing of "DFAST" technology for POD encryption and host decryption is one way to place such content protection terms and conditions on host devices. That approach will support content providers' delivery of important categories of programming and viewing options to the digital television market.

In response to the Commission's recent invitation to comment (NPRM at 9), we believe that Circuit City's assertion that this licensing model is inappropriate is erroneous. That assertion is technologically unsound because it fails to recognize that content protection in the host is necessary as a practical matter; terminating content protection with the expiration of the cable operators' access control in the POD, as Circuit City appears to assert, amounts to no content protection at all. Because of retail separation, neither content providers nor cable operators can ensure content protection within the host device. And even if content protection could somehow be imposed at the outputs of host devices,⁵ content would remain subject to misuse by such

⁵As discussed below, even if that were possible, Circuit City's position would lead to a
(continued...)

devices, misdirection - such as to the Internet - from them, and interception for misuse from within them. The assertion is also unprincipled, because it has no basis whatsoever in the Commission's rationale for separating security and navigation (namely, insulating cable operator's business from intrusion by independent manufacturers).

Most fundamentally, Circuit City's assertion that this model is not consistent with "relevant Commission rules" (NPRM at 10) and that content protection conditions cannot be imposed on host devices, is incorrect. The Commission itself has explicitly stated: "'copy protection' systems and devices that impose a limited measure of data encryption control over the types of devices that may record (or receive) video content would not be subject to the separation requirement." In the Matter of Implementation of Section 304/Navigation Devices, FCC 97-80 at ¶ 63. Indeed, were Circuit City correct, myriad individual content providers and cable operators could deliver uniquely encrypted content requiring widely varying decryption facilities for digital television to reach a fragmented audience. Such a non-uniform approach could not have been the Commission's purpose.

As the Commission recognizes, there are several currently unresolved issues pending in negotiations between affected parties over the terms and conditions to be recognized and accepted, by manufacturers and content owners alike, in content protection technology licenses across the POD interface and over 1394 connections - two components of adequate and effective content protection discussed earlier. MPAA Member Companies are diligently pursuing with other interested parties regular, intense negotiations to resolve these issues. In the interim, final development and deployment of device implementations has not been hindered. DTCP chips (for 1394 content protection) and development licenses for POD-host interface implementation of DFAST are readily available.

We do not believe the Commission can effectively determine by rulemaking what levels of risk should be accepted by content owners, or what "price" (restrictions on use generally) should be paid for third-party technology. Nor does the Commission have the authority to regulate private contracts in this matter. As a general principle, American regulatory law gives paramount importance to private contracts, which control the arrangements between the parties unless a compelling public interest justifies government intervention. Additionally, a rulemaking approach is likely to assure contention and delay that is unnecessary in view of private sector discussions that already have made substantial progress.

C. Non-Premium Digital Services

The Commission also asked whether a POD module will be needed in order to receive packages of non-premium services; and whether to permit scrambling in such cases. Again, the terms under which individual content providers may deliver programming should be a matter for

⁵(...continued)
fragmented, non-uniform result that could not be in the public interest.

individual decision. But the framework answer is: yes; the ability to scramble, and hence the need for a POD (as well as the conditions we have urged for "cable-ready" labeling and the possible need for disclosures of limitations on capabilities of certain receivers) must apply to non-premium services. Individual content providers may decide, for example, that content offered on non-premium tiers should be scrambled across a POD interface in order to restrain digital serial copying or unauthorized Internet retransmission.

The existing (waivable) prohibition on "scrambl[ing] or otherwise encrypt[ing] signals carried on the basic service tier" (47 CFR 76.630) was adopted, as the Commission recognizes, "in the analog domain" (NPRM text at n. 36), and with regard to existing cable and consumer equipment (Id. at 36-37). Additionally, it dealt with conditional access of consumers to cable services; it did not consider the need for post-reception content protection within and among new devices in the digital era. As noted earlier, the Commission has explicitly recognized the need for encryption or scrambling to provide content protection. FCC 97-80, supra. For all the reasons discussed earlier, this prohibition - and the need for individual waivers - should not apply to encryption or scrambling for content protection purposes within and among digital devices.

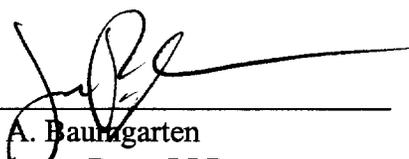
* * * *

Date: May 24, 2000

Respectfully submitted,

MOTION PICTURE ASSOCIATION
OF AMERICA, INC.

By:



Jon A. Baumgarten
Proskauer Rose, LLP
1233 20th Street, N.W., Suite 800
Washington, D.C. 20036
202/416-6800
jbaumgarten@proskauer.com
Counsel for MPAA