

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

In the Matter of

Digital Broadcast Copy Protection

)  
)  
)  
)  
)  
)

MB Docket No. 02-230

**JOINT COMMENTS OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., ABC, ABC TELEVISION AFFILIATES ASSOCIATION, AFMA, AMERICAN ASSOCIATION OF ADVERTISING AGENCIES, AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS, AMERICAN SOCIETY OF COMPOSERS, AUTHORS AND PUBLISHERS, ASSOCIATION FOR MAXIMUM SERVICE TELEVISION, INC., ASSOCIATION OF NATIONAL ADVERTISERS, INC., BELO CORP., BROADCAST MUSIC, INC., CBS, DIRECTORS GUILD OF AMERICA, FOX BROADCASTING COMPANY, INTERNATIONAL ALLIANCE OF THEATRICAL AND STAGE EMPLOYEES, MOTION PICTURE TECHNICIANS, ARTISTS AND ALLIED CRAFTS OF THE UNITED STATES, ITS TERRITORIES AND CANADA, AFL-CIO, CLC, NATIONAL ASSOCIATION OF BROADCASTERS, SCREEN ACTORS GUILD, INC., WRITERS GUILD OF AMERICA, EAST, INC., AND WRITERS GUILD OF AMERICA, WEST, INC.**

Jon A. Baumgarten  
Bruce E. Boyden  
Proskauer Rose LLP  
1233 Twentieth Street NW, Suite 800  
Washington, DC 20034  
(202) 416-6800

Mace J. Rosenstein  
Jacqueline P. Cleary  
Hogan & Hartson LLP  
555 Thirteenth Street NW  
Washington, DC 20004  
(202) 637-5600

December 6, 2002

*Counsel for The Motion Picture Association  
of America, Inc.*

## **SUMMARY**

Because it is transmitted in the clear, digital broadcast television is subject to an extraordinarily high risk of unauthorized redistribution over networks such as the Internet. The threat of such wide-scale piracy, if not addressed, will lead content providers to cease making their high-value programming available over broadcast television. The DTV transition would be seriously threatened by such a development, with consequent harm to consumers.

The Commission must therefore implement the proposed regulations attached to these Joint Comments mandating protection of digital broadcast television in a few types of consumer products. These proposed regulations are based upon the cross-industry discussions that occurred in the Broadcast Protection Discussion Group. The Broadcast Flag is the most appropriate and efficient solution for the protection of digital broadcast television. The Flag, however, should not be required to be embedded in content, in the event that a content provider wishes to make its broadcast content available for wide redistribution.

The Broadcast Flag solution regulates a minimum number of products. Products containing modulators or demodulators would be directly subject to the Requirements for the Protection of Unencrypted Digital Terrestrial Broadcast Content Against Unauthorized Redistribution (the "Requirements"). Demodulators are the most appropriate gateway to commence protection, because prior to demodulation the content is not in usable form; after demodulation, the content may be in usable form. Regulation of modulators is necessary in order to prevent other content protection systems from being undermined by the very rules necessary to protect digital broadcast television content.

The Commission must also regulate a limited number of products that are capable of receiving protected but unprocessed content, or digital broadcast content passed in a certain way

within a computer. Such products would only be subject to the regulation if their manufacturers file a written commitment with the Commission to abide by the Requirements. Once a commitment has been filed, such products would become eligible to protect unprocessed content or content passed within a computer by using a self-certified protection method. The Commission would administer and enforce this process. Equipment used by satellite, cable, and other professional retransmitters of digital broadcast content is exempt from the Requirements. However, such retransmitters would be required to ensure that retransmitted digital broadcast content is protected once received by the consumer's set-top box.

The Commission should authorize a list of specified protection technologies, known as "Table A," for use with digital broadcast content.<sup>1</sup> Without such a list, manufacturers would lack guidance concerning implementation of the Requirements and disputes over their implementation would inevitably arise. Given the ever-changing nature of technology, objective criteria specifying certain features for protection technologies may quickly become obsolete; instead, the Commission should adopt flexible, market-based criteria for Table A technologies, to be administered by the Commission.

The Broadcast Flag solution will have minimal impact on consumers. Consumers will still be able to distribute and record protected digital broadcast content within the personal digital network environment, defined as the home or similar local environment. Furthermore, implementation of the Broadcast Flag solution will have no impact on existing consumer equipment. The cost impact on affected equipment going forward will be insignificant.

---

<sup>1</sup> The National Association of Broadcasters has not endorsed the criteria for selection or the procedures for admission to Table A and has formed no position on this issue.

The Commission has jurisdiction to adopt the proposed regulations. The Commission has express statutory authority under 47 U.S.C. § 336 to adopt rules to prevent unauthorized redistribution of digital terrestrial broadcast television programming. Furthermore, the Commission has ancillary jurisdiction to adopt such rules under Titles I and III of the Communications Act. Given the fact that protection of digital broadcast content is necessary to implement a robust DTV transition, the Commission has ample authority to act under existing legislation.

TABLE OF CONTENTS

|   | <u>Page</u> |
|---|-------------|
| SUMMARY .....   | i           |
| INTRODUCTION  | 1           |
| I. THE BROADCAST FLAG SOLUTION IS NECESSARY IN ORDER TO FACILITATE THE DTV TRANSITION.....  | 6           |
| A. Unlike Other Digital Programming Distribution Methods, Digital Broadcast Television Is Subject to an Extraordinarily High Risk of Unauthorized Redistribution..... | 6           |
| B. Without Protection Against Unauthorized Redistribution, the Viability of Distribution of High-Value Broadcast Programming Will Be Seriously Undermined.....        | 8           |
| II. THE COMMISSION SHOULD ADOPT THE BROADCAST FLAG SOLUTION TO PREVENT UNAUTHORIZED REDISTRIBUTION OF DIGITAL BROADCAST CONTENT.....                                  | 10          |
| A. Regulations Are Necessary in Order to Implement the Broadcast Flag Solution.   | 10          |
| B. There Are No Technical Impediments to Implementation of the Broadcast Flag Solution.....   | 11          |
| C. The Broadcast Flag Is the Most Appropriate Technological Model to Be Used..  | 11          |
| D. Authorized Technologies Will Be Upgraded and Improved Upon Over Time. ...  | 11          |
| E. The Broadcast Flag Solution Should Be Implemented As Soon As Possible.....   | 12          |
| F. The Broadcast Flag Solution Will Create and Maintain Industry Incentives to Continually Innovate to Improve the Method of Digital Content Protection. ....         | 12          |
| III. A MANDATE TO BROADCASTERS AND CONTENT PROVIDERS TO EMBED THE BROADCAST FLAG IS UNNECESSARY AND UNDULY RESTRICTIVE.....   | 13          |
| IV. THE BROADCAST FLAG SOLUTION REGULATES A MINIMUM NUMBER OF DEVICES.....  | 14          |
| A. The Commission Must Mandate That Products Containing Demodulators or Modulators Comply With the Broadcast Flag Requirements.....                                   | 14          |

|      |   |    |
|------|---|----|
| B.   | Demodulation Is the Most Appropriate Point to Commence Protection of Digital Broadcast Content. ....  | 15 |
| C.   | The Commission Must Mandate That a Limited Set of Products Other Than Modulators and Demodulators Comply With the Broadcast Flag Requirements. ....                                       | 16 |
| D.   | Cable or Satellite Systems Would Be Required to Ensure Protection of Retransmitted Digital Broadcast Content. ....  | 18 |
| V.   | THE COMMISSION SHOULD AUTHORIZE A LIST OF TECHNOLOGIES FOR PROTECTION OF DIGITAL BROADCAST CONTENT USING FLEXIBLE, MARKET-BASED CRITERIA. ....  | 19 |
| A.   | The Authorization of Specific Protection Technologies Is Critical to the Broadcast Flag Solution. ....  | 19 |
| B.   | The Commission Should Adopt the Market-Based Criteria Attached to These Joint Comments. ....  | 20 |
| C.   | Responsibility for Making Determinations to Authorize Protection Technologies Should Rest With the Commission Staff. ....   | 24 |
| VI.  | THERE ARE NO PRIVACY CONCERNS OR CONSTITUTIONAL ISSUES RAISED BY THE BROADCAST FLAG SOLUTION. ....  | 24 |
| A.   | There Are No Privacy Concerns Raised By the Broadcast Flag Solution. ....   | 24 |
| B.   | There Are No Constitutional Issues Raised By the Broadcast Flag Solution. ....  | 25 |
| VII. | THE BROADCAST FLAG SOLUTION WILL HAVE MINIMAL IMPACT ON CONSUMERS. ....   | 25 |
| A.   | The Broadcast Flag Solution Will Not Interfere With Consumers’ Ability to Make Secure Copies of DTV Content Within the Personal Digital Network Environment. ....                         | 25 |
| B.   | DTV Broadcast Content Should Be Protected From Unauthorized Redistribution of Unencrypted Digital Terrestrial Broadcast Content Outside of the Personal Digital Network Environment. .... | 26 |
| C.   | The Broadcast Flag Solution Will Not Affect Consumers’ Existing Equipment, and Will Not Impede the Development of New Consumer Technologies. ....   | 27 |
| D.   | The Broadcast Flag Solution Will Have No Significant Cost Impact on Affected Consumer Equipment. ....   | 28 |

|       |   |    |
|-------|---|----|
| VIII. | THE COMMISSION HAS AUTHORITY TO REGULATE THE<br>RETRANSMISSION OF DIGITAL BROADCAST VIDEO CONTENT IN<br>ORDER TO PROTECT THE INTEGRITY OF FREE, OVER-THE-AIR<br>BROADCAST TELEVISION. ....  | 29 |
| A.    | The Commission has Express Statutory Authority to Adopt Rules to<br>Prevent the Unauthorized Redistribution of Digital Terrestrial Broadcast<br>Television Programming. ....  | 29 |
| B.    | The Promulgation of Rules Designed to Prevent the Unauthorized<br>Redistribution of Digital Terrestrial Broadcast Television Programming<br>Would Be “Reasonably Ancillary” to the Commission’s Jurisdiction under<br>Titles I and III of the Act. .... | 32 |

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

**In the Matter of**

**Digital Broadcast Copy Protection**

)  
)  
)  
)  
)  
)

**MB Docket No. 02-230**

**JOINT COMMENTS OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., ABC, ABC TELEVISION AFFILIATES ASSOCIATION, AFMA, AMERICAN ASSOCIATION OF ADVERTISING AGENCIES, AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS, AMERICAN SOCIETY OF COMPOSERS, AUTHORS AND PUBLISHERS, ASSOCIATION FOR MAXIMUM SERVICE TELEVISION, INC., ASSOCIATION OF NATIONAL ADVERTISERS, INC., BELO CORP., BROADCAST MUSIC, INC., CBS, DIRECTORS GUILD OF AMERICA, FOX BROADCASTING COMPANY, INTERNATIONAL ALLIANCE OF THEATRICAL AND STAGE EMPLOYEES, MOTION PICTURE TECHNICIANS, ARTISTS AND ALLIED CRAFTS OF THE UNITED STATES, ITS TERRITORIES AND CANADA, AFL-CIO, CLC, NATIONAL ASSOCIATION OF BROADCASTERS, SCREEN ACTORS GUILD, INC., WRITERS GUILD OF AMERICA, EAST, INC., AND WRITERS GUILD OF AMERICA, WEST, INC.**

The Motion Picture Association of America, Inc. (“MPAA”), ABC, ABC Television Affiliates Association, AFMA, American Association of Advertising Agencies (“AAAA”), American Federation of Television and Radio Artists (“AFTRA”), American Society of Composers, Authors and Publishers (“ASCAP”), Association for Maximum Service Television, Inc. (“MSTV”), Association of National Advertisers, Inc. (“ANA”), Belo Corp., Broadcast Music, Inc. (“BMI”), CBS, Directors Guild of America (“DGA”), Fox Broadcasting Company (“FBC”), International Alliance of Theatrical and Stage Employees, Motion Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada, AFL-CIO, CLC (“IATSE”), National Association of Broadcasters (“NAB”), Screen Actors Guild, Inc. (“SAG”),

Writers Guild of America, East, Inc. (“WGA-East”), and Writers Guild of America, West, Inc. (“WGA-West”) hereby submit these Joint Comments in response to the Commission’s Notice of Proposed Rulemaking in the above-captioned proceeding.<sup>2</sup>

Appended to these Joint Comments at Attachments A through D are documents comprising and describing a specific proposal for regulations that the Commission should adopt to protect digital broadcast television content against unauthorized redistribution. Attachment A, a White Paper entitled “A Proposal for Protection of Unencrypted Digital Broadcast Television,” provides a plain-language description of the proposed regulation. Attachment B, entitled “Requirements for the Protection of Unencrypted Digital Terrestrial Broadcast Content Against Unauthorized Redistribution,” sets forth the regulatory requirements compliant consumer products would be subject to. Attachment C, entitled “Proposal for Table A Criteria,” contains a proposal for criteria the Commission would use to authorize technologies for use as protected digital outputs or protected recording methods. Attachments B and C, in addition to receiving the support of most of the signatories of these Joint Comments (with the exceptions noted herein), are also supported by the Digital Transmission Licensing Administrator, LLC (commonly known as “5C”), as indicated in its separately filed comments. Finally, Attachment D sets forth the form of the list of authorized technologies, referred to herein as “Table A.”

The parties submitting these Joint Comments represent a wide variety of content owners, producers, and distributors. The MPAA is a nonprofit trade association representing seven of the largest producers and distributors of feature films, television programs and home video entertainment material. The members of the MPAA include Sony Pictures Entertainment Inc.,

---

<sup>2</sup> See Notice of Proposed Rulemaking, FCC 02-231, M.B. Docket No. 02-230 (rel. Aug. 9, 2002).

Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Twentieth Century Fox Film Corporation, Universal City Studios, Inc., Warner Bros., and an affiliate of The Walt Disney Company.

Founded in 1917, the AAAA is the national trade association representing the American advertising agency business. Its nearly 600 members, comprised of virtually all of the large, multi-national agencies and hundreds of small and mid-sized agencies, maintain 2,000 offices throughout the country. Together, AAAA member agencies represent about 75 percent of all national, regional and local advertising placed by agencies in the United States.

ABC, CBS, and FBC provide news, sports, and entertainment programming to their broadcast affiliates and their owned and operated television stations.

The ABC Television Affiliates Association is an organization that represents the interests of the local television stations that are affiliated with the ABC Television Network, but not commonly owned with the Network.

The AFMA (formerly known as the American Film Marketing Association) is a trade association representing more than 150 independent producers and distributors of motion pictures and television programming, including Cinetel Films, Inc., ECG Worldwide Entertainment, Intermedia, Lions Gate Films International, Miramax International, New Concorde Pictures, New Line Cinema, and RKO Pictures. AFMA's members produce more than 400 independent motion pictures and countless hours of diverse television programming annually.

AFTRA is a national labor union affiliated with the AFL-CIO that is headquartered in New York City with 36 local offices throughout the country, representing members in four major areas: 1) news and broadcasting; 2) entertainment programming; 3) the recording business; and

4) commercials and non-broadcast, industrial, educational media. AFTRA's 80,000 members are seen or heard on television, radio and sound recordings and include actors, announcers, news broadcasters, singers (including royalty artists and background singers), dancers, sportscasters, disc jockeys, talk show hosts and others. Talent payments under AFTRA contracts are over \$1 billion a year.

ASCAP and BMI represent American composers, lyricists and music publishers. BMI and ASCAP license the right of nondramatic public performance of the copyrighted musical compositions created and owned by their members and affiliates, as well as the members of 60 affiliated foreign performing rights licensing organizations. Among their licensees are United States broadcast television stations and networks. ASCAP and BMI join in these Joint Comments because the regulatory regime detailed in these Joint Comments will protect against unauthorized and infringing performances of the copyrighted musical compositions in their repertoires which are contained in broadcast television programming. ASCAP and BMI were not involved in the determination of the proper technical means to protect television content as described in these Joint Comments. They support the suggestions of the owners of copyrighted program content set forth in these Joint Comments as to the technical means to achieve such protection.

ANA is the industry's premier trade association dedicated exclusively to marketing and brand building. Representing more than 300 companies with 8,000 brands that collectively spend over \$100 billion in marketing communications and advertising, the Association's members market products and services to consumers and businesses. ANA serves the needs of its members by providing marketing and advertising industry leadership in traditional and e-

marketing, legislative advocacy, information resources, professional development and industry-wide networking.

Belo Corp., based in Dallas, is one of the nation's largest media companies with a diversified group of market-leading television, newspaper, cable and interactive media assets.

DGA represents 12,700 directors and members of the directorial team who work in feature film, filmed, taped, and live television, commercials, documentaries, and news. Members include Directors, Unit Production Managers, Assistant Directors, Associate Directors, Technical Coordinators, Stage Managers, and Production Associates. DGA serves as the exclusive collective bargaining representative for these individuals.

IATSE is the labor union representing technicians, artisans and craftpersons in the entertainment industry including live theatre, film and television production and trade shows. In the United States, IATSE has approximately 107,000 members.

MSTV is a non-profit trade association representing the television broadcast industry. MSTV's primary focus is in areas of new digital technologies and the efficient use of broadcast spectrum.

NAB is a nonprofit, incorporated association of television and radio stations and broadcasting networks that serves and represents the American broadcast industry.

The SAG is the collective bargaining representative for over 96,000 professional actors and performing artists, including dancers, singers, and stunt performers, in the theatrical and television motion picture industry.

The WGA-East is a labor organization and the exclusive collective bargaining representative for approximately 4,500 professional authors of stories and screenplays for theatrical and television motion pictures and interactive technologies. The WGA-East also

represents news writers for radio and television. Writers represented by the WGA-East perform writing services throughout the United States east of the Mississippi.

The WGA-West is a labor organization and the exclusive collective bargaining representative for approximately 8,500 professional authors of stories and screenplays for theatrical and television motion pictures and interactive technologies. The WGA-West also represents news writers for radio and television. Writers represented by the WGA-West perform writing services throughout the United States west of the Mississippi.

I. THE BROADCAST FLAG SOLUTION IS NECESSARY IN ORDER TO FACILITATE THE DTV TRANSITION.

A. Unlike Other Digital Programming Distribution Methods, Digital Broadcast Television Is Subject to an Extraordinarily High Risk of Unauthorized Redistribution.

¶3. *Q. In light of the importance placed upon digital broadcast copy protection by some industry participants, and with a view towards facilitating the DTV transition, this Notice seeks comment on whether a regulatory copy protection regime is needed within the limited sphere of digital broadcast television. As an initial matter, we seek comment on whether quality digital programming is now being withheld because of concerns over the lack of digital broadcast copy protection. In particular, we seek comment on the nature and extent of the piracy concerns expressed by content providers. If such programming is being withheld, will it continue to be withheld in the absence of a regulatory regime?*

A regulatory redistribution control regime<sup>3</sup> is essential in order to protect digital broadcast television content and facilitate a meaningful DTV transition. Unlike other digital

---

<sup>3</sup> We refer throughout these comments to a “redistribution control regime” rather than a “copy protection regime” because the Broadcast Flag solution is designed only to prevent unauthorized redistribution of digital broadcast television content outside the home or other similar local environment. The Broadcast Flag solution does not prevent copies from being made within the home. It requires that such copies be sufficiently secure so as to prevent unauthorized redistribution outside the home being accomplished from those copies.

programming distribution methods such as cable, satellite, or DVDs, digital broadcast television is transmitted in the clear, and thus is subject to an extraordinarily high risk of unauthorized redistribution. Once received in the home, digital broadcast television content can easily be redistributed via retransmission over networks like the Internet by such means as rebroadcasting, hosting files on a web server, or peer-to-peer file trafficking. Such unauthorized redistribution can be accomplished without downloading any special software, without the need for circumventing any copy protections, without such tools as analog-to-digital converters, or indeed without any complex technical skills whatsoever. For example, all a person has to do is to select “Record” while watching TV on his or her computer using a TV tuner card, and then save the file to a publicly accessible folder on his or her hard drive, where it can be illegally redistributed to anonymous users via peer-to-peer file trafficking. Or that person can easily e-mail the file as an attachment to an unlimited number of people. Or he or she can simply place the recorded file on a personal webpage for unauthorized redistribution to others on the Internet. The capability of the Internet to allow distribution worldwide, instantly, to millions of recipients, distinguishes the looming threat of digital piracy from previous technologies, such as the VCR, that rely on the creation and distribution of physical copies. With worldwide unauthorized redistribution of digital content so easy to accomplish, the threat of widespread piracy is enormous, even if the number of pirates is low. Any recipient of digital broadcast television, not just the professional pirate or amateur hacker, would have it within his or her power to illegally redistribute digital broadcast television content almost at will, everywhere on Earth.

Without a regulatory redistribution control regime, content providers are faced with the spectre of digital piracy on a massive scale of whatever content they make available for digital broadcast. Given the extent of such piracy, it would be impossible to combat the unauthorized

retransmission of digital content effectively merely by pursuing individual infringement actions. Rather, a comprehensive regulatory framework must be established to ensure the protection of digital broadcast content as it enters consumer products. Otherwise, as broadcast television transitions into the digital era and as broadband capacity expands, we can expect that producers of compelling programming will recalculate their interest in licensing their most valuable content over a distribution mechanism so easily susceptible to unauthorized redistribution, and will consider instead limiting such programming to more secure channels such as conditional access systems.<sup>4</sup> As one studio has noted in a letter cited by the Commission, without regulatory action, in the future “broadcast content will be relegated to second-class status.” *See In the Matter of Digital Broadcast Copy Protection*, FCC 02-231 at 1 n.1.

B. Without Protection Against Unauthorized Redistribution, the Viability of Distribution of High-Value Broadcast Programming Will Be Seriously Undermined.

*Q. To what extent would the absence of a digital broadcast copy protection scheme and the lack of high quality digital programming delay or prevent the DTV transition? Would the resulting dynamic threaten the viability of over-the-air television? What impact would this have on consumers?*

The DTV transition may be seriously threatened if, due to the threat of piracy, valuable programming ceases to be available for broadcast. The loss of compelling programming free of charge via broadcast television would also heavily affect consumers. Broadcast television is a unique resource, justly cherished by millions of Americans. It has been a staple of American culture since the 1950s. In addition to its importance domestically, broadcast television

---

<sup>4</sup> The GAO has noted that concerns over unauthorized copying and retransmission may act as a disincentive to offering digital content over digital broadcast television. *See U.S. General Accounting Office, Additional Federal Efforts Could Help Advance Digital Television*

programming is a major United States export that is tremendously important both to the American economy and to our prestige in the world. For all of these reasons, broadcast television is a critically important resource that must be preserved.

High-value broadcast programming exists only because of the market foundation on which it has been built. A multi-billion dollar industry, employing thousands of individuals, broadcast television depends on an economic model that relies not on fees collected from the individual consumer, but on advertising revenue and on profits from resale rights both here and abroad. Under this model, broadcast television content providers have invested millions of dollars in producing expensive, high-quality, high-production-value programming. This programming could not exist without the expectation of the revenue generated by sales of advertisements in particular geographic markets and by syndication of programs after their initial broadcast. Content owners, directors, writers, actors, distributors, and others all depend on the existence of that revenue stream for their compensation and their ability to produce and distribute new works.

The viability of the economic model upon which the broadcast television industry is built will be seriously undermined by rampant piracy if digital broadcast television content is not protected. Unauthorized redistribution would inflict enormous damage on both of the pillars upon which broadcast television now stands. It would cripple advertising revenue by hindering broadcast content providers' ability to distribute content on a territorial basis and to adapt advertising to particular markets; and it would seriously damage critically important resale and syndication rights.

The result could be the destruction of broadcast television programming as we currently know it. The loss of valuable programming via free, over-the-air broadcast television would reduce the rich range of options consumers presently have in choosing the means of viewing valuable content. Indeed, poorer consumers who may not be able to afford conditional access subscription fees may be shut out of obtaining quality television programming entirely, a consequence that would exacerbate fears of the emergence of a “two-tiered” information society.

II. THE COMMISSION SHOULD ADOPT THE BROADCAST FLAG SOLUTION TO PREVENT UNAUTHORIZED REDISTRIBUTION OF DIGITAL BROADCAST CONTENT.

A. Regulations Are Necessary in Order to Implement the Broadcast Flag Solution.

¶4. *Q. If a digital broadcast flag or other regulatory regime is needed, we seek comment on whether the Commission should adopt rules or create some other mechanism to resolve outstanding compliance, robustness and enforcement issues.*

The Commission should adopt rules implementing the Broadcast Flag solution as agreed upon by the cross-industry Broadcast Protection Discussion Group and as initially drafted in the Requirements document contained at Tab C-1 of the BPDG Final Report, and as since refined in Attachment B to these Joint Comments. No other mechanism would be as comprehensive or effective in implementing the regulatory regime. The Commission should further adopt rules to resolve any outstanding compliance, robustness, and enforcement issues. The signatories to these Joint Comments have proposed a set of rules, annexed at the Attachments, to address all remaining outstanding issues.

B. There Are No Technical Impediments to Implementation of the Broadcast Flag Solution.

*Q. We also seek comment on whether there are any technical impediments to implementation of a digital broadcast copy protection scheme.*

There are no technical impediments to implementation of the Broadcast Flag solution. Indeed, implementation of the Broadcast Flag will bring digital television into an already existing framework of content protection; and unlike other such schemes, the Broadcast Flag itself is royalty free. Once the solution is adopted, the incentive will exist for the creation of an even more rich and diverse population of output and recording protection technologies, which will ensure that all product manufacturer and consumer needs are met. While four such technologies have gained sufficient marketplace approval to qualify as authorized technologies under the Compliance and Robustness Requirements, several others are in development that have the potential to be equally effective.

C. The Broadcast Flag Is the Most Appropriate Technological Model to Be Used.

*Q. We ask commenters to elaborate on whether the ATSC flag is the appropriate technological model to be used, or whether there are alternatives to the ATSC flag. We seek comment on the effectiveness of any such technological model in protecting digital broadcast content from improper redistribution.*

There are no alternatives to the ATSC flag that accomplish the protection of digital broadcast content in such an economical and practical manner. The Broadcast Flag solution requires fewer resources in the equipment than other possible solutions, and is thus the most efficient solution for both the product manufacturer and the consumer.

D. Authorized Technologies Will Be Upgraded and Improved Upon Over Time.

*Q. For example, we seek comment on the technological robustness of the ATSC flag and whether it can be upgraded or improved upon over time.*

The Broadcast Flag itself is completely adequate for its purpose and will not require any updating. It is envisioned that the technological implementation of the Compliance and Robustness Requirements, on the other hand, will be upgraded and improved upon over time. Under the criteria for authorized technologies contained in the Attachment, technologies with sufficient marketplace support can be authorized and listed on Table A. Additions to Table A can (and are expected to) be constantly made over time. Finally, procedures will be created to remove a technology from Table A that has been significantly compromised. Thus, the list of authorized technologies will evolve to meet changing circumstances.

E. The Broadcast Flag Solution Should Be Implemented As Soon As Possible.

*Q. If the ATSC flag is the best means of protection currently available, but it still has technical flaws, is it better to mandate the flag now and monitor it as technology develops, or to wait until a more effective means of digital broadcast copy protection is developed?*

There are no technical flaws with the Broadcast Flag solution; the solution is sound and ready for implementation. The cost of delay, on the other hand, is as described previously: the longer digital broadcast television remains unprotected in the face of the development of other, secure distribution channels, the greater the threat to the digital television transition and even the future viability of free, over-the-air broadcast itself.

F. The Broadcast Flag Solution Will Create and Maintain Industry Incentives to Continually Innovate to Improve the Method of Digital Content Protection.

*Q. Would a regulatory copy protection regime create and maintain industry incentives to continually innovate to improve the method of digital content protection?*

Technology manufacturers would have the incentive to continually improve and advance their technologies in order to capture as large a portion of the digital broadcast content protection market as possible. As already noted, the list of authorized technologies for the protection of digital broadcast television content would not be static; rather, under the criteria proposed by the MPAA and others, any manufacturer whose technology is able to receive sufficient marketplace support, or is at least as effective as a technology that has already been authorized, may be listed as an authorized technology. Innovation is thus certain to continue unabated under the Broadcast Flag solution.

Similarly, the Broadcast Flag solution will not, in itself, interfere in any way with continued innovation in the development of open source software. While building a secure open source protection technology will no doubt be a challenge, it is a challenge faced by open source programmers in developing *any* secure application, not just Authorized Digital Output Protection Technologies or Authorized Recording Methods. We welcome the efforts of open source programmers to meet this challenge and develop secure digital output protection technologies and recording methods for submission for inclusion on Table A.

III. A MANDATE TO BROADCASTERS AND CONTENT PROVIDERS TO EMBED THE BROADCAST FLAG IS UNNECESSARY AND UNDULY RESTRICTIVE.

¶5. *Q. With respect to the type of Commission regulations that would be appropriate in the digital broadcast copy protection area, we seek comment on whether broadcasters and content providers should be required to embed the ATSC flag or another type of content control mark within digital broadcast programming, or whether they have sufficient incentive to protect such programming such that a government mandate is unnecessary.*

The presence of the ATSC flag means that redistribution control is being asserted. The flag distinguishes material as to which technological redistribution control is being asserted from

material, without the flag, as to which the content provider may be asserting no technological redistribution control at all. Content providers will generally embed the flag in their high-value programming, including films and first-run series, for all the reasons stated above concerning the threat of piracy. Requiring the presence of the flag in all digital broadcast television content, however, may unduly restrict some content providers from making selected programs freely available for redistribution. Some content providers may decide that some of their programming need not be protected from redistribution in order to preserve its value. For example, a small digital broadcast television station may wish one of its local programs to be “simulcast” by viewers over the Internet. Mandatory embedding of the flag would unnecessarily prevent such redistribution even where permitted by the content owner.

#### IV. THE BROADCAST FLAG SOLUTION REGULATES A MINIMUM NUMBER OF DEVICES.

##### A. The Commission Must Mandate That Products Containing Demodulators or Modulators Comply With the Broadcast Flag Requirements.

¶6. *Q. On the reception side, we seek comment on whether the Commission should mandate that consumer electronics devices recognize and give effect to the ATSC flag or another type of content control mark. If so, we seek comment on whether this mandate should include devices other than DTV broadcast receivers and what the resulting impact would be on consumers. More specifically, the BPDG Final Report anticipates that digital broadcast copy protection will begin at the point of demodulation.*

An effective comprehensive solution must be mandated by the Commission for pertinent products. (Although the Commission’s Notice refers to “consumer electronic devices,” it is essential, and we assume the Commission intended, that computer or “IT” products be regulated, as well as so-called “CE” products.) Under the proposal as contained in the BPDG Final Report and the Attachments to these Joint Comments, only products containing demodulators or

modulators<sup>5</sup> will be directly subject to the Commission’s mandate. Certain other products -- “Downstream Products,” as described below -- will be subject to the Commission’s mandate only if the product manufacturer voluntarily agrees to bind itself to comply with the Requirements by participating in a “written commitment” to do so.<sup>6</sup> Computers and other general purpose products may thus elect not to commit to comply with the Requirements, and in that case may continue to serve other purposes but may not receive flagged digital broadcast content. Regulation of Downstream Products is necessary to ensure that the written commitments are in fact honored, that the Requirements are enforced against manufacturers of downstream products that have made the commitment, and that non-participating products do not receive protected content. Without regulation of Downstream Products, product manufacturers would have reduced flexibility to design modular products.

B. Demodulation Is the Most Appropriate Point to Commence Protection of Digital Broadcast Content.

*Q. We seek comment on whether this is an appropriate point for digital broadcast copy protection to begin in consumer electronics devices.*

Demodulation is the most appropriate gateway at which to commence protection. Prior to demodulation, the digital broadcast television signal is in an unusable, modulated form. After demodulation and transport stream processing, the digital broadcast television signal is in readily

---

<sup>5</sup> Regulation of consumer products with modulators is necessary in order to prevent other content protection systems from being undermined by the very rules necessary to protect digital broadcast television content. Without regulation of modulators, under the Requirements, content that originated in another protected distribution channel, such as view-only content distributed over a broadband connection, or encrypted pay-per-view transmissions, could be mislabelled as copyable digital broadcast content and redistributed using compliant products.

usable form, and thus subject to copying and redistribution. While demodulated but unprocessed content is currently unusable by most consumers, such content if exposed may in the future become more susceptible to unauthorized redistribution, thus also leaving a fertile field for piracy. Enacting protections to take effect only at some point subsequent to demodulation and transport stream processing would be pointless, as the damage would have been done by that point. Regulation at the point of demodulation is therefore critical to the success of the Broadcast Flag solution. That is why Section X.13 in Attachment B regulates all demodulators.

C. The Commission Must Mandate That a Limited Set of Products Other Than Modulators and Demodulators Comply With the Broadcast Flag Requirements.

*Q. We also seek comment on whether and how downstream devices would be required to protect the content.*

In order for the Broadcast Flag solution to be complete, downstream products receiving a digital signal must protect against unauthorized redistribution. Under the Requirements, a product “downstream” from the product containing the demodulating device can receive digital television content in one of three principal ways:<sup>7</sup> (1) the product may receive content protected by an Authorized Digital Output Protection Technology; (2) the product may be a “Downstream Product,” as that term is defined in Section X.1 of the Requirements; or (3) the product may receive content over an analog output.

---

<sup>6</sup> See the Attachments for a proposed description of the nature of the “written commitment”.

<sup>7</sup> In addition to these three principal methods, the product may also receive content: where the source product maintains sole control over access to the content; via a consumer modulator compliant with the Requirements; via a certain type of constrained DVI output; and in order to make a recording using an Authorized Recording Method.

In the case of a product receiving content over an analog output, no restrictions are imposed by the Requirements. In the case of a product receiving content protected by an Authorized Digital Output Protection Technology, the product would generally not be subject to the Requirements, but would be subject to any licensing terms imposed by the manufacturer of the authorized output protection technology. Consideration of the protection offered by such license terms is a critical part of the procedure for gaining admission to Table A.

“Downstream Products” are a narrow subset of products whose manufacturers have filed a “written commitment” to subject themselves to the Requirements. Upon filing the written commitment, the manufacturer’s product becomes eligible to receive protected but unprocessed digital television content or protected content passed within a computer, provided that the connection uses a “Robust Method” meeting specified standards. The Robust Method need not be identified on Table A nor authorized for this limited purpose by the Commission. The purpose of the Downstream Products definition is to allow product manufacturers, if they wish, to separate demodulation from transport stream processing among different products and to allow computer manufacturers flexibility in designing after-market add-in products. Although it does not perform demodulation, the Downstream Product would be required to protect digital broadcast television content in exactly the same manner as products containing source (demodulating) devices — by complying with the Compliance and Robustness Requirements. The Demodulator Compliance Requirements (Sections X.3 through X.6) restrict the types of outputs and recording methods that may be employed by a product handling protected digital television content. The Demodulator Robustness Requirements (Sections X.7 through X.11) require products to meet a specified level of secure construction, e.g., by employing encryption techniques and by being tamper-resistant. Both the Compliance and Robustness Requirements

are essential for Downstream Products as well as products containing source (demodulating) devices in order to protect against unauthorized redistribution.<sup>8</sup>

D. Cable or Satellite Systems Would Be Required to Ensure Protection of Retransmitted Digital Broadcast Content.

*Q. In addition, we seek comment on whether and how an ATSC flag or other system would work for broadcast stations carried on cable or direct broadcast satellite systems.*

The Requirements apply only to “Unencrypted Digital Terrestrial Broadcast Content” -- content broadcast “without encrypting or otherwise making the content available through a technical means of conditional access.” However, digital broadcast content should also be protected when retransmitted by cable or satellite systems. The Requirements thus protect digital broadcast content that is modulated in 64- or 256-QAM by a cable system and retransmitted in unencrypted form; such content becomes subject to the Requirements upon demodulation by the consumer’s set-top box. Other retransmitters, however, such as direct broadcast satellite systems, not only use a variety of changing modulation methods not readily specified in the Requirements, but also encrypt retransmitted broadcast television signals, making it impossible to check such signals for the Flag until they are decrypted. In order to ensure that retransmitted digital broadcast television content is protected, the proposed Requirements attached hereto provide that retransmitters that encrypt digital broadcast television signals must ensure that

---

<sup>8</sup> The Requirements also include a provision that Table A technologies must check for the Flag in unscreened content, or require other products to do so. Similar to the provisions governing consumer modulators, this requirement is necessary in order to prevent other content protection systems from being undermined by the rules proposed here. Without such a requirement, content that originated in another protected distribution channel, such as view-only content distributed over a broadband connection, or encrypted pay-per-view transmissions, could be mislabelled as copyable digital broadcast content and redistributed using compliant products.

digital broadcast content marked with the Broadcast Flag is protected, either by checking for the flag themselves at the head end and requiring protection by the consumer set-top box, or requiring the set-top box to check for the Broadcast Flag upon decryption of the signal. If the Broadcast Flag is determined to be present, the retransmitter must require the consumer set-top box or other receiving product to abide by the Requirements as if it contained a covered demodulation function.

The Requirements also create an exemption for demodulation and modulation devices sold to satellite, cable, or other professional services. Such equipment would not be subject to the Requirements, provided that the satellite or cable system file a written commitment that it will abide by the requirement specified above to ensure protection of digital broadcast content in its subscribers' set-top boxes.

V. THE COMMISSION SHOULD AUTHORIZE A LIST OF TECHNOLOGIES FOR PROTECTION OF DIGITAL BROADCAST CONTENT USING FLEXIBLE, MARKET-BASED CRITERIA.

A. The Authorization of Specific Protection Technologies Is Critical to the Broadcast Flag Solution.

¶7. *Q. As to the means by which digital broadcast copy protection would be achieved, we seek comment on whether to require the use of specific copy protection technologies, such as those identified in Table A to the BPDG Final Report, in consumer electronics devices.*

One of the key provisions of the Compliance and Robustness Requirements proposal, see the Attachment, Sections X.3(a)(3), X.3(b)(2), X.4(a)(3), X.4(b)(2), is that digital outputs and recording methods in source products and Downstream Products be generally protected by any authorized technologies to prevent unauthorized redistribution. The authorized technologies will

be those listed on Table A.<sup>9</sup> It is important to note that the list of authorized technologies on Table A will not be static; new technologies may be continually added as they are developed, and technologies that are substantially compromised may be removed from the list, thus allowing for innovation and changed circumstances.

It is a crucial part of the Broadcast Flag solution that consumer electronics and computer product manufacturers<sup>10</sup> in most instances be required to use one or more of the Table A technologies in designing the digital outputs and recording methods of their products. Without such a requirement, there would be no guidance to product manufacturers as to what technologies to include, insufficient certainty concerning the standards to be met, and unavoidable contention between content providers and manufacturers concerning the meaning of the Requirements. Such an environment would be antithetical to the DTV transition, and would necessarily involve the Commission in constant adjudicatory actions.

B. The Commission Should Adopt the Market-Based Criteria Attached to These Joint Comments.

*Q. Table A identifies those copy protection technologies considered by BPDG for use in conjunction with digital outputs in consumer electronics devices, such as Digital Transmission Content Protection (“DTCP” or “5C”) or High-Bandwidth Digital Content Protection (“HDCP”). However, BPDG members were unable to agree on the criteria by which a copy protection technology would be evaluated and approved for digital broadcast use and chose to reserve the topic*

---

<sup>9</sup> As noted earlier, in some cases, connections *between* a product containing a demodulation device and a Downstream Product must comply with specified robustness standards but need not be identified on Table A. Similarly, in certain cases where recordings are technologically bound to play back on that recording device, such binding may be accomplished by a technology that is not identified on Table A. See Attachment, Sections X.3(b)(1) and X.4(b)(1).

<sup>10</sup> As noted earlier, we assume that by “consumer electronic devices” the Commission intends to refer both to stand-alone consumer products as well as computer-related equipment. Both types of products are encompassed by the Requirements.

*for potential further discussion by a CPTWG parallel group. We seek comment on how a particular technology would receive approval for use in consumer electronics devices for digital broadcast copy protection purposes.*

The parties submitting these Joint Comments propose a set of criteria and procedures for admission to Table A (the “Table A Proposal”)<sup>11</sup> (attached to these Joint Comments at Attachment C) based upon the joint proposal submitted to the BPDG by MPAA member companies, Computer Industry Group companies, and 5C companies. The Table A Proposal represents a fair and balanced approach to determining which technologies are authorized for protection of digital television content. Instead of locking in technological mandates that may quickly become obsolete, or abstract concepts that offer little guidance, the Proposal adopts a flexible, market-based approach under which a technology is authorized for Table A if it has been accepted in the relevant marketplace as a protection technology or it is just as effective as one that has. The Proposal contains fair and carefully balanced procedures for continually adding new technologies to the list. This method of protecting outputs and recordings ensures that innovation in the product manufacturing industry continues unabated. Continued innovation not only benefits technology manufacturers and consumers, but also content providers, who will benefit most of all from the creation of a continually evolving list of state-of-the-art technologies for content protection.

The Table A Proposal includes several procedures to determine if a technology has been accepted in the marketplace. If a technology provider believes its technology meets one of the criteria, it may file an application stating the grounds for its belief. The companies named in the application as having “used or approved” the technology in the market would then be requested

---

<sup>11</sup> NAB has not endorsed the criteria for selection or the procedures for admission to Table A and has formed no position on this issue.

to respond; if the companies do not respond to the request, they will be deemed to have admitted the facts alleged in the application. Any remaining dispute would be fairly but swiftly resolved by Commission staff.

The Table A Proposal recognizes that the terms of many technology and content licenses may not be public, and that therefore the proponent of a new technology may feel it needs further information to determine whether its technology is being “used or approved” in the marketplace. The Table A Proposal therefore includes a procedure by which a technology provider may file a notice seeking more information from one or more companies concerning their “use or approval” of its technology. The companies named in the notice would be required to respond to this request.

The Table A Proposal also recognizes that some Table A technologies may be compromised. Therefore, to protect against inevitable hacks, the Table A Proposal includes a procedure by which a request can be made to remove a technology from Table A if it has been compromised. The procedure would allow interested parties to object to the request for removal. The Commission would then make a timely determination as to whether or not such technology should be removed from Table A. In doing so, the Commission would consider two factors: the protection of digital television against unauthorized redistribution, and the impact on content owners, consumers and manufacturers resulting from the continued use of the compromised technology and from any removal of the technology from the list.

While appropriately respectful of marketplace decisions, the Table A Proposal also includes a safeguard provision under which Commission staff may determine that the marketplace has been unreasonably slow in adopting a proposed technology that is just as effective as a technology already on Table A. The safeguard provision is intended to address any

concerns about the fairness of market-based criteria. Indeed, the procedures for this safeguard provision, set forth as Section X.14(a)(2) of the Table A Proposal, are more detailed than any other procedure contained in the Proposal. Under the safeguard provision, the proponent of a new technology that is “at least as effective” as a technology already on Table A may apply to have it added to the list. The Commission will issue a public notice providing 60 days for comment on the request to place the technology on Table A. If three or more major content providers object, Commission staff will resolve the matter through an expedited process, not to exceed 45 additional days. The staff will consider not only the effectiveness of the proposed technology in protecting digital television content from unauthorized redistribution, but also any applicable license terms of the technology relating to security, enforcement, and updates.

Although the proposed regulations attached hereto at the Attachment do not identify particular technologies that should be added to Table A upon enactment, it is important that the Commission act immediately upon issuing these regulations to simultaneously identify appropriate technologies to be admitted to Table A. Swift approval of an initial set of technologies is necessary to facilitate the digital television roll-out, to protect digital broadcast television content as soon as the regulations become effective, and to inform manufacturers of the technical means of implementing the Broadcast Flag solution.

We believe that the above criteria and procedures represent a flexible and fair solution that carefully balances the interests of content providers, purveyors of technology, product manufacturers, and the public, because they reflect the actual marketplace experience of affected market sectors, with the extra safeguard that additional technologies can be added even without any marketplace acceptance if other criteria are met.

C. Responsibility for Making Determinations to Authorize Protection Technologies Should Rest With the Commission Staff.

*Q. We also seek comment on identifying the appropriate entity to make an approval determination.*

The procedures identified in the Table A Proposal depend on administration and oversight by a neutral body that would have the authority and the expertise to conduct hearings and investigations and make determinations concerning whether the criteria have been met, and whether a technology has been compromised. While the MPAA member companies have not yet conferred with the other parties to the proposal to decide what body should administer the criteria, we believe that the most appropriate body would be the Commission staff (but with respect to removal from Table A, the proposal requires action by the full Commission).<sup>12</sup>

VI. THERE ARE NO PRIVACY CONCERNS OR CONSTITUTIONAL ISSUES RAISED BY THE BROADCAST FLAG SOLUTION.

A. There Are No Privacy Concerns Raised By the Broadcast Flag Solution.

¶8. *Q. We also seek comment on the extent to which broadcast copy protection technologies raise privacy concerns and whether rules are needed to ensure that consumers' privacy interests are protected.*

Neither the Broadcast Flag nor the Compliance and Robustness Requirements raise any privacy concerns. The Broadcast Flag solution does not require the reporting of any information from the consumer electronics or computer product to locations outside the personal digital network environment; therefore no privacy concerns are implicated by this solution.

---

<sup>12</sup> NAB has not concluded whether the most appropriate body to make approval determinations for Table A is the Commission staff as proposed in these Comments by MPAA, a due process industry body, or some other means.

B. There Are No Constitutional Issues Raised By the Broadcast Flag Solution.

*Q. In addition, we seek comment on whether there are First Amendment or any other constitutional issues that we should consider from the point of view of the industries involved or individual consumers.*

There are no First Amendment or other constitutional issues raised by the Broadcast Flag solution. The Broadcast Flag is not unlawfully compelled speech. Nor do the Requirements impose an unconstitutional burden on manufacturers. As has been done in the past with the All Channels Receiver Act and the V-Chip statute, manufacturers may be required to comply with certain standards for a legitimate public policy purpose. Nor are the speech rights of consumers affected by the Broadcast Flag solution. Consumers will continue to have the right to speak and debate in just as many fora after the solution is implemented. Nothing in the Requirements will prevent consumers in any way from commenting upon, speaking about, and debating the thoughts and ideas they receive via digital television, or from sharing new thoughts and ideas with others.

VII. THE BROADCAST FLAG SOLUTION WILL HAVE MINIMAL IMPACT ON CONSUMERS.

A. The Broadcast Flag Solution Will Not Interfere With Consumers' Ability to Make Secure Copies of DTV Content Within the Personal Digital Network Environment.

¶9. *Q. Finally, we seek comment on the impact of the ATSC flag or other digital broadcast copy protection mechanism on consumers. The BPDG Final Report asserts that a broadcast flag system would not interfere with consumers' ability to make secure copies of DTV content for their personal use, either on personal video recorders or removable media. Similarly, the BPDG Final Report states that the requirements to protect digital outputs should not interfere with consumers' ability to send DTV content across secure digital networks, such as "home digital network connecting digital set top boxes, digital recorders, digital servers and digital display devices." We seek comment on these assertions.*

The Broadcast Flag solution as envisioned in the Requirements is designed to prevent unauthorized redistribution outside of the personal digital network environment. As noted above, it is not a form of digital broadcast copy protection. The Requirements do not place restrictions on analog copying; for example, the Requirements will have no impact on the use of VCRs. With respect to digital copying, the Requirements allow the creation of digital recordings using authorized recording methods, and allow transmission between products using authorized digital outputs. Indeed, the technologies that MPAA member companies have thus far recognized as satisfying the criteria for Table A — DTCP, HDCP, CPRM, and D-VHS — all allow secure digital transmission and recording within the personal digital network environment. We expect that future technologies will also satisfy the criteria in a similar manner.

B. DTV Broadcast Content Should Be Protected From Unauthorized Redistribution of Unencrypted Digital Terrestrial Broadcast Content Outside of the Personal Digital Network Environment.

*Q. We also seek comment on the appropriate scope of protection to be accorded DTV broadcast content.*

The goal of the Broadcast Flag solution is to prevent unauthorized redistribution of unencrypted digital terrestrial broadcast content outside of the personal digital network environment. “Personal digital network environment” means the home or similar local environment. The “home” consists of all the rooms or areas within a consumer’s primary residence. “Similar local environment” expands beyond the limited definition of “home” to include locations such as a consumer’s car, boat, RV, or second home. “Personal digital network environment” thus covers any of these types of locations, but does not cover unauthorized or insecure transmission between or among them. That is, the Broadcast Flag solution allows for a

flexible definition of “personal digital network environment” to include electronic transmission of digital broadcast content between various locations typically associated with a consumer’s home, but quite reasonably does not require content owners to accept unauthorized transmissions or intolerably low levels of security. Nor does the Broadcast Flag technology itself limit a consumer’s ability to make or move physical copies of broadcast content.

With respect to security, technologies to securely bind content to the personal digital network as it is being transferred between or among locations do not exist today. We invite and encourage the development of such technologies that could expand consumer choice so long as content owners’ valuable rights in their content are protected.

C. The Broadcast Flag Solution Will Not Affect Consumers’ Existing Equipment, and Will Not Impede the Development of New Consumer Technologies.

*Q. In addition, some parties have raised concerns about the potential impact of a broadcast flag requirement on consumers’ existing and future electronic equipment. We seek comment on these concerns, as well as the potential effect of a broadcast flag requirement on the development of new consumer technologies.*

The Broadcast Flag requirement will have no impact on consumers’ existing equipment. The Broadcast Flag itself is merely a message in the ATSC stream that is fully compatible with current ATSC-compliant devices. The Broadcast Flag solution will not prevent consumers’ existing equipment from displaying or recording content marked with the flag. Since analog outputs are a permitted output under the Requirements, existing analog displays, players, and recorders will continue to function with the new compliant products under the Compliance and Robustness Requirements. Furthermore, the restrictions imposed by the Requirements on digital outputs will hardly be unusual considering existing private contractual agreements for the protection of conditional access television and other forms of content. Enactment of the

Requirements will ensure that digital broadcast television is protected in a similar fashion as with every other form of digital audiovisual content, but without the limitations on copying that other protection arrangements may impose. Moreover, secure copies will be viewable on the playback facility of the recorder that made them. Thus, any incidental incompatibility between secure recordings and legacy players will commonly involve distribution of the recording to other persons or locations. In order to achieve a balanced solution, however, this incidental legacy issue must not be used to undermine needed security of freely permitted copies.

As noted, the Broadcast Flag will in no way retard the development of new consumer technologies. Under the criteria for Table A, any technology that has achieved marketplace acceptance, or that is at least as effective as a technology already on Table A, can be added to Table as an authorized technology. We envision that Table A will grow to include a diverse population of authorized technologies as competing technology manufacturers vie to capture more market share. Four such technologies have already gained sufficient industry acceptance to qualify as authorized technologies, while several others are in development that have the potential to be equally effective.

D. The Broadcast Flag Solution Will Have No Significant Cost Impact on Affected Consumer Equipment.

*Q. Finally, we seek comment on the cost impact, if any, that a broadcast flag requirement would have on affected consumer electronics equipment.*

The cost impact on affected products of implementing the Broadcast Flag requirement will be insignificant. Already, several technologies worthy of listing on Table A exist in the marketplace, even without the Broadcast Flag requirement, thus proving that such technologies are both affordable and readily available. The vast majority of products will also record, process,

and display pay television and other types of content that will require such technologies be implemented even without the Broadcast Flag requirement. In addition, many products are already manufactured under private licensing arrangements that are very similar to the Compliance and Robustness Requirements. The existence of such products is additional proof that the cost impact of the Broadcast Flag requirement will be negligible.

VIII. THE COMMISSION HAS AUTHORITY TO REGULATE THE RETRANSMISSION OF DIGITAL BROADCAST VIDEO CONTENT IN ORDER TO PROTECT THE INTEGRITY OF FREE, OVER-THE-AIR BROADCAST TELEVISION.

*Q. We seek comment on the jurisdictional basis for Commission rules dealing with digital broadcast television copy protection. Is this an area in which the Commission could exercise its ancillary jurisdiction under Title I of the Act? We ask commenters to identify provisions of the Act that provide the Commission with authority to implement its ancillary jurisdiction. If the Commission has ancillary jurisdiction over digital broadcast copy protection, are there any limits upon its scope? For example, does the Commission have authority to mandate the recognition of the ATSC flag in consumer electronics devices? We also ask commenters to identify any statutory provisions that might provide the Commission with more explicit authority to adopt digital broadcast copy protection rules. For example, do Sections 336(b)(4) and (b)(5) impact upon the Commission's ability to adopt digital broadcast copy protection regulations?*

A. The Commission has Express Statutory Authority to Adopt Rules to Prevent the Unauthorized Redistribution of Digital Terrestrial Broadcast Television Programming.

The Telecommunications Act of 1996 added a new Section 336 to the Communications Act, expressly delegating to the FCC broad authority to implement a nationwide system of over-the-air digital broadcast television. 47 U.S.C. § 336. Subsection 336(b)(4) directed the Commission, in order to carry out its digital mandate, to “adopt such technical and other requirements as may be necessary or appropriate to assure the quality of the signal used to provide advanced television services.” 47 U.S.C. § 336(b)(4). Concurrently, Congress enacted a

new subsection 336(b)(5), which authorizes the Commission to “prescribe such other regulations as may be necessary for the protection of the public interest, convenience and necessity.”

47 U.S.C. § 336(b)(5).

Both individually and together, these statutory provisions, which were intended to facilitate the creation of an efficient nationwide system of digital broadcast television, confer on the Commission the authority to take such actions as it deems necessary to advance the public interest in the context of the digital transition. Indeed, the ranking members of the House Committee on Energy and Commerce during the 107th Congress underscored the Commission’s broad authority under its digital mandate when, citing 47 U.S.C. § 336(b)(4) and (5), they emphasized that “[t]he FCC currently possesses the authority” under these provisions to adopt rules providing for digital redistribution protection.<sup>13</sup>

There can be no dispute that the public interest would be served by rules designed to prevent the unauthorized redistribution of programming initially distributed *via* free, digital terrestrial broadcast television.<sup>14</sup> Absent such rules, the availability of high quality digital content to broadcast television stations would be severely limited – at best – in favor of more

---

<sup>13</sup> See Letter to Chairman Michael K. Powell, Federal Communications Commission, from Representative W.J. “Billy” Tauzin, Chairman, and Representative John D. Dingell, Ranking Member, House Committee on Energy and Commerce (July 19, 2002) (“Tauzin/Dingell Letter”) at 1-2; Letter to Chairman Michael K. Powell, Federal Communications Commission, from Sen. Ernest F. Hollings, Chairman of the Senate Commerce, Science and Transportation Committee (July 19, 2002) (“Hollings Letter”) at 2-3.

<sup>14</sup> The preservation of a viable free, over-the-air broadcast service historically has been, and remains, a fundamental objective of Congress and of this Commission. See, e.g., H.R. CONF. REP. NO. 106-464, at 101 (1999) (“Congress’ interest in maintaining free over-the-air television will be undermined if local broadcasters are prevented from reaching viewers by either cable or satellite distribution systems.”); H. R. REP. NO. 102-628, at 51 (1992) (“The absence of local signal carriage requirements will result in a weakening of the over-the-air television industry and a reduction in competition, thereby depriving the public of those benefits.”); S. REP. NO. 102-92, at 62 (1991) (“Without congressional action, the Committee concludes that the role of local

secure channels such as conditional access systems. Failure to adopt protection technology comprehensively and across all distribution modalities would impede the development and availability of free, over-the-air digital television, contravening the Congressional mandate expressly embodied in Section 336 of the Act.

The Commission historically has regulated various characteristics of television reception equipment in order to ensure the integrity of the terrestrial broadcast television system. The Commission has, for example, prescribed rules that (i) ensure that television receivers are capable of receiving all over-the-air television channels (47 C.F.R. § 15.117(b)); (ii) require television set manufacturers to provide an equivalent antenna for the reception of UHF channels as that provided for VHF channels (47 C.F.R. § 15.117(e)); (iii) establish maximum noise figures and picture sensitivity standards (47 C.F.R. §§ 15.117(f) and (g)); (iv) require television sets to be capable of displaying closed captions (47 C.F.R. § 15.119); and (v) require the incorporation of technology to permit blocking of certain programming based on content (“v-chip” technology) (47 C.F.R. § 15.120). As these provisions and others demonstrate,<sup>15</sup> the Commission has not hesitated to adopt rules affecting equipment manufacturers where to do so was necessary to promote the public interest in the efficient, nationwide delivery of broadcast service.<sup>16</sup> The instant circumstances are no different.

---

television broadcasting in our system of communications will steadily decline[.]”).

<sup>15</sup> Express statutory authority has not been a prerequisite for the promulgation of rules pertaining to the manufacture of television reception equipment. For example, the Commission adopted the NTSC standard governing the transmission and reception of color television signals in the absence of an explicit statutory mandate. *See Amendment of the Commission’s Rules Governing Color Television Transmissions*, 41 FCC 658 (1953).

<sup>16</sup> More recently, the Commission acted pursuant to 47 U.S.C. § 303(s) to require that equipment manufacturers include digital tuner sections in certain new television receivers on a phased-in schedule, beginning in 2004. *See Review of the Commission’s Rules and Policies Affecting the Conversion to Digital Television*, 17 FCC Rcd 15978 (2002).

Accordingly, in order to avoid clearly disadvantageous outcomes for broadcasters and viewers alike, and to discharge its mandate to ensure the efficient and timely transition to digital broadcasting, the Commission has authority under Section 336 generally, and under subsections 336(b)(5) and 336(b)(4) in particular, to mandate the implementation of protections against unauthorized redistribution of digital terrestrial broadcast programming.<sup>17</sup>

B. The Promulgation of Rules Designed to Prevent the Unauthorized Redistribution of Digital Terrestrial Broadcast Television Programming Would Be “Reasonably Ancillary” to the Commission’s Jurisdiction under Titles I and III of the Act.

Even assuming, *arguendo*, the absence of the express statutory mandate embodied in Section 336, the Commission’s authority over matters “reasonably ancillary” to its jurisdiction under Title I and Title III of the Act, and its fundamental statutory duty to ensure the viability of free, over-the-air television, empower it to adopt rules designed to prevent the unauthorized redistribution of digital broadcast content.

The Communications Act confers upon the Commission the broad authority to “perform any and all acts, make such rules and regulations, and issue such orders . . . as may be necessary in the execution of its functions.” 47 U.S.C. § 154(i). The Act separately provides that the Commission may, in the broadcast context, “[m]ake such rules and regulations and prescribe such restrictions . . . as may be necessary to carry out the provisions of this Act . . . .” 48 U.S.C. § 303(r).

---

<sup>17</sup> The Commission previously recognized the importance of protecting digital video content from unauthorized redistribution when it held that its rules pertaining to navigation devices do not preclude cable operators from requiring equipment manufacturers to incorporate protection technology into their products. *See Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, 15 FCC Rcd 18199, 18209, 18211-12 (2000) (Commission will “take appropriate action” to ensure that the implementation of redistribution protection technology across different sectors does not disadvantage one industry participant vis-à-vis others, to the detriment of copyright holders and,

In enacting the Communications Act, Congress intended “to confer upon the Commission sweeping authority to regulate ‘in a field of enterprise the dominant characteristic of which was the rapid pace of its unfolding.’” *Office of Communication of the United Church of Christ v. FCC*, 707 F.2d 1413, 1423 (D.C. Cir. 1983) (quoting *National Broadcasting Co. v. United States*, 319 U.S. 190, 219 (1943)). The Act was intended to be a “supple instrument for the exercise of discretion by the expert body which Congress has charged to carry out its legislative policy.” *FCC v. Pottsville Broadcasting Co.*, 309 U.S. 134, 138 (1940). The Commission, as the “single Government agency with ‘unified jurisdiction’ and ‘regulatory power over all forms of . . . communication,’” therefore, is granted “broad authority” to fulfill its regulatory responsibilities. *U.S. v. Southwestern Cable Co.*, 392 U.S. 157, 167-68 (1968) (quoting legislative history of the Act) (footnotes omitted).<sup>18</sup>

A federal regulatory agency is authorized to promulgate regulations in the absence of an express delegation of power so long as the regulations at issue are reasonably necessary to advance the purpose of the agency’s enabling legislation. *See, e.g., Interstate Commerce Commission v. American Trucking Associations*, 467 U.S. 354, 356, 364-70 (1984) (“*ATA IP*”) (upholding ICC action because it was “closely and directly related to the [ICC’s] express statutory powers and [was] designed to achieve” statutory objectives); *Whirlpool Corp. v. Marshall*, 445 U.S. 1, 9-13 (1980) (upholding agency regulation because it furthered the

---

indirectly, the public).

<sup>18</sup> *See also Capital Cities Cable, Inc. v. Crisp*, 467 U.S. 691, 700 (1984); *Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1162 (D.C. Cir. 1995); *United Video, Inc. v. FCC*, 890 F.2d 1173, 1182-83 (D.C. Cir. 1989); *NARUC v. FCC*, 746 F.2d 1492, 1499, 1501 (D.C. Cir. 1984); *Wold Communications, Inc. v. FCC*, 735 F.2d 1465, 1474-76 (D.C. Cir. 1984).

overriding purpose of OSHA even though not expressly authorized by statute). This maxim of statutory interpretation dates back over half a century.<sup>19</sup>

In one of the seminal cases enunciating the doctrine of ancillary jurisdiction, *Interstate Commerce Commission v. American Trucking Associations*, 344 U.S. 298 (1953) (“*ATA I*”), the Supreme Court concluded that the ICC could regulate the use of non-owned equipment by motor carriers even in the absence of an express statutory delegation of authority to do so. 344 U.S. at 309. Recognizing that “nowhere in the [Motor Carriers] Act is there an express delegation of power to control, regulate or affect leasing practices” and that “in each separate provision of the Act granting authority there is no direct implication of such power,” the Supreme Court nonetheless concluded that its analysis should not end “among the literal words of the statutory provisions.” *Id.* Indeed, the Court explicitly rejected the notion that Congress, in delegating agency powers, can, as a practical matter, embody within such delegation the full scope of the authority it means to prescribe. *Id.* at 309-10. Rather, it held that because the purpose of the rules under review was “to protect the industry from practices detrimental to the maintenance of sound transportation services consistent with the regulatory system,” the ICC had the authority to enact them. *Id.* at 310-12.

---

<sup>19</sup> See *United States v. Pennsylvania R.R. Co.*, 323 U.S. 612, 615-19 (1945). See also *United States v. Southwestern Cable Co.*, 392 U.S. 157, 177 (1968) (FCC has “ancillary jurisdiction” over CATV systems in order to discharge its statutory mandate to facilitate the development of a nationwide system of local television broadcasting); *United States v. Midwest Video Corp.* (“*Midwest Video I*”), 406 U.S. 649, 668-70 (1972) (upholding FCC’s program-origination rule under ancillary jurisdiction doctrine); *In re Trans Alaska Pipeline Rate Cases*, 436 U.S. 631, 633, 651-56 (1978) (ICC has authority ancillary to statutory suspension power to establish maximum interim rates and refund provisions); *United States v. Chesapeake & Ohio Ry. Co.*, 426 U.S. 500, 513-15 (1976) (upholding ICC accounting order as “a legitimate, reasonable, and direct adjunct to the Commission’s explicit statutory power to suspend rates pending investigation”); *In re Permian Basin Area Rate Cases*, 390 U.S. 747, 774-77 (1968) (upholding Federal Power Commission’s jurisdiction over prices charged by field producers

The principles set forth in *ATA I* apply equally to this Commission’s authority over television broadcasting in general, and the transition to digital broadcast television in particular. Thus, the Supreme Court has recognized that the Commission has authority over matters “reasonably ancillary to the effective performance of [its] various responsibilities for the regulation of television broadcasting.” *U.S. v. Southwestern Cable Co.*, 392 U.S. at 178. In *Southwestern Cable*, the Commission promulgated rules imposing requirements on cable television system operators in the absence of an express statutory delegation of jurisdiction. The assumption of jurisdiction by the Commission in *Southwestern Cable* was based on its concern that “the likelihood or probability of [CATV’s] adverse impact upon potential and existing [broadcast] service has become too substantial to be dismissed.” *Id.* at 165 (citations omitted). The Commission feared that cable systems’ “importation of distant signals into the service areas of local stations also may ‘destroy or seriously degrade the service offered by a television broadcaster,’ and thus ultimately deprive the public of the various benefits of a system of local broadcasting stations.” *Id.* at 175 (citation omitted). In upholding the Commission’s assertion of jurisdiction, the Supreme Court embraced the Commission’s determination that its “regulatory authority over CATV is imperative if it is to perform with appropriate effectiveness certain of its other responsibilities.” *Id.* at 173.

The potential harms at issue here raise precisely the type of issue that confronted the Commission in *Southwestern Cable*: uncontrolled, unauthorized redistribution of content delivered *via* digital terrestrial broadcast television will directly and adversely affect the quality and level of service provided by broadcasters to the public. In *Southwestern Cable*, the Commission regulated the importation of distant broadcast signals by cable systems and imposed

---

pursuant to its statutory authority to regulate interstate transportation).

certain non-duplication requirements on cable systems in order to protect broadcast stations from audience erosion – and, in turn, the viability of free, over-the-air television. The Supreme Court found these aspects of cable regulation were sufficiently related to broadcasting that they fell within the ambit of the Commission’s jurisdiction, notwithstanding the lack of an express Congressional grant of authority to regulate cable systems. Protecting the integrity of digital broadcast transmissions, by definition, relates directly to broadcasting and therefore falls squarely within the Commission’s jurisdiction; moreover, as in *Southwestern Cable*, the availability of quality programming *via* free, over-the-air television will be adversely affected in the absence of Commission action.

The Supreme Court has recognized and endorsed the Commission’s jurisdiction not only to take action to protect television broadcasting, but also, more generally, to advance the underlying policy imperatives of the Communications Act. In the case the D.C. Circuit has called a “giant step beyond *Southwestern [Cable]* in relaxing the nature of the ancillarity necessary to support an assertion of Commission power . . .”, *NARUC v. FCC*, 533 F.2d 601, 616 (D.C. Cir. 1976), the Supreme Court agreed that the FCC had jurisdiction to impose local program origination requirements on cable systems because the regulation served the same purposes as analogous requirements applicable to broadcast stations. *U.S. v. Midwest Video Corp.*, 406 U.S. 649 (1972). Precisely because broadcasters and viewers alike will suffer direct adverse consequences if the Commission does not act to prevent the unauthorized retransmission of over-the-air digital broadcast signals – in contrast to the admittedly attenuated relationship between broadcasting and the regulation of local program origination on cable systems – the

Commission may assert jurisdiction over this matter without taking even a single step beyond the *Southwestern Cable* doctrine.<sup>20</sup>

In *Southwestern Cable*, the Supreme Court cited decisions in which it had determined that the Court “may not, ‘in the absence of compelling evidence that such was Congress’ intention . . . prohibit administrative action imperative for the achievement of an agency’s ultimate purposes.’” *Southwestern Cable*, 392 U.S. at 177-78 (quoting *Permian Basin Area Rate Cases*, *supra*, 390 U.S. at 780 (elision in original)). Here, Congressional leaders have emphasized that the Commission “has ample authority to address [issues relating to the digital television transition] independently of the Congress.”<sup>21</sup> The ranking members of the House Committee on Energy and Commerce in the 107<sup>th</sup> Congress have stated that “Title I of the Communications Act

---

<sup>20</sup> The doctrine on which the Supreme Court relied in *Southwestern Cable* has been applied repeatedly since that decision. *See, e.g., Midwest Video I*, 406 U.S. 649, 668-70 (1972); *Computer & Communications Indus. Ass’n v. FCC*, 693 F.2d 198, 213 (D.C. Cir. 1982) (upholding FCC’s ancillary jurisdiction over carrier-provided enhanced services and CPE in order to assure wire services at reasonable rates); *CBS, Inc. v. FCC*, 629 F.2d 1, 26-27 (D.C. Cir. 1980) (alternatively holding that FCC’s application of Section 312(a)(7) to networks was an exercise of power reasonably ancillary to the effective enforcement of the statutory provision), *aff’d*, 453 U.S. 367 (1981). *See also ACLU v. FCC*, 523 F.2d 1344, 1350-01 (9th Cir. 1975) (upholding promulgation of regulations pertaining to cable television under ancillary jurisdiction doctrine); *Mt. Mansfield Television, Inc. v. FCC*, 442 F.2d 470, 487 (2d Cir. 1971) (adoption of syndicated exclusivity rule “‘reasonably ancillary to the effective performance of the [FCC’s] various responsibilities for the regulation of television broadcasting’”) (quoting *Southwestern Cable*, 392 U.S. at 178). *Cf. Home Box Office, Inc. v. FCC*, 567 F.2d 9, 25-34 (D.C. Cir. 1977) (FCC did not have ancillary jurisdiction to promulgate pay cable rules because it did not “demonstrate that the objectives to be achieved by regulating cable television [were] also objectives for which the Commission could legitimately regulate the broadcast media”); *National Ass’n of Regulatory Util. Comm’rs v. FCC*, 533 F.2d 601, 611-17 (D.C. Cir. 1976) (FCC’s preemption of state regulation of the use of cable system leased access channels for two-way, point-to-point, non-video communications was improper because not sufficiently related to its jurisdiction over broadcasting and FCC was barred from regulating intrastate common carrier activities).

<sup>21</sup> *See* Tausin/Dingell Letter at 1; Hollings Letter at 2.

provides [the Commission with] jurisdiction that is ‘reasonably ancillary’ to its specific grants of authority over telecommunications issues.’<sup>22</sup>

That Congress may independently consider whether to codify the Commission’s ancillary authority to prevent unauthorized retransmission of digital broadcast matter does not preclude a finding that the Commission possesses such authority today.<sup>23</sup> The Court addressed precisely this issue in *Southwestern Cable*, where certain parties had urged the Court to infer from the Commission’s efforts to obtain legislation expressly establishing its jurisdiction over cable television systems that the Commission lacked authority to regulate cable systems. 392 U.S. at 170. Although, at the time, a bill expressly conferring jurisdiction had been introduced in the Senate, Congress ultimately failed to enact it. *Id.* at 164, 171. The Court, however, explained that the meaning to be divined from the *absence* of congressional action was far from self-evident: “Congress may well have been more troubled about the Commission’s unwillingness to regulate than by any fears that it was unable to regulate,” the Court stated. *Id.* at 171. This is precisely the scenario presented today. Congressional leaders have indicated that, although they may in the future pursue legislation to address the issue of digital content redistribution, they believe the FCC already has authority to act “independently of the Congress.”<sup>24</sup>

To be sure, in some cases courts have held that certain regulatory actions can exceed the scope of a Congressional mandate. But the clear theme of such cases is that the agency attempted to promulgate regulations that *contradicted* express statutory provisions or bore no meaningful relation to (or affirmatively frustrated) Congress’ objectives.

---

<sup>22</sup> Tauzin/Dingell Letter at 1. *See also* Hollings Letter at 2-3.

<sup>23</sup> *See* Tauzin/Dingell Letter at 1-2; Hollings Letter at 2.

<sup>24</sup> Tauzin/Dingell Letter at 1. *See also* Hollings Letter at 2.

Thus, for example, in *Motion Picture Association of America, Inc. v. FCC*, 309 F.3d 796 (D.C. Cir. 2002), the D.C. Circuit reversed and vacated the Commission’s order adopting video description rules on the bases that (i) in cases where the FCC implements “regulations that significantly implicate content, Sec. 1 [of the Act] is not a source of authority.” *Id.* at 798-99, 802-06; (emphasis added) and (ii) the legislative history of the 1996 Act made clear that Congress did not intend to confer upon the Commission the authority to adopt regulations requiring video description. *Id.* The Court went on to distinguish the broad jurisdiction delegated to the Commission by Congress under Section 1 of the Act with respect to non-content based regulations – citing *United States v. Southwestern Cable Co.* – from the narrow and express delegation of authority that is a prerequisite for adoption of content-based regulations. The D.C. Circuit’s conclusion that the Commission exceeded its authority by adopting content-based regulations in the absence of an express statutory delegation of authority (and in the face of clear legislative history to the contrary) pursuant to Section 1 of the Act does not affect the analysis of the Commission’s jurisdiction to adopt rules to protect digital broadcasts from unauthorized redistribution. In fact, the D.C. Circuit’s decision confirms the Commission’s “broad” authority under Section 1 to adopt non-content-based regulations. *Id.* at 804-05.<sup>25</sup> Unlike audio descriptions of video programming, which necessarily require the injection of new content into programming, the Broadcast Flag protects the integrity of transmissions without affecting the content embodied within them.

---

<sup>25</sup> The Commission also has recently reaffirmed its willingness to rely on ancillary jurisdiction. In its *Report and Order, Compatibility Between Cable Systems and Consumer Electronics Equipment*, the Commission relied on jurisdiction ancillary to its statutory labeling authority to promulgate labeling standards for digital television receivers. See 15 FCC Rcd 17568, 17576 (¶ 23) (2000).

Similarly, in *Midwest Video II* the Court concluded that the FCC did not have authority under a theory of ancillary jurisdiction to promulgate rules requiring cable television systems over a certain size to provide third parties access to certain channels and to furnish them equipment and facilities for access purposes. 440 U.S. at 709. The Court distinguished the rules it had upheld in *Midwest Video I* by explaining that they required cable television systems affirmatively to advance certain broadcast policy objectives in light of their efforts to “[enmesh themselves] in the field of television broadcasting.” *Id.* at 700. The *Midwest Video II* Court reasoned that, unlike the program-origination rules imposed on CATV systems in *Midwest Video I*, the access rules at issue in this case impinged on cable operators’ editorial discretion. *Id.*

And, in the *NARUC* case, the court determined that the FCC did not have jurisdiction to preempt state and local regulation of the use of cable system leased access channels for two-way, non-video communications. 533 F.2d at 615, 617. At the outset of its analysis, the court stated that it had “great difficulty” identifying any purpose related to broadcasting that would be served by the rules under review; indeed, the court explained, because of “the private nature of the non-video, return communications involved,” it was difficult for it to see how action by the Commission “could have as its primary impact the furtherance of any broadcast purpose,” or even any *indirect* ways in which the rules might further any broadcast purpose. *Id.* at 615-16. In the event, the rules ran headlong into a statutory restraint on the Commission’s jurisdiction. *Id.* at 617. Specifically, the Act barred the Commission from exercising jurisdiction over the type of intrastate common carrier activities at issue in the case. *Id.* at 617.

Viewed against this backdrop, it is clear that, in implementing rules to prevent the unauthorized retransmission of digital broadcast matter, the Commission would not be taking extraordinary action, or assuming jurisdiction over issues that are not central to the rollout of

digital television, or acting in a manner inconsistent with the express will of the Congress. To be sure, if this were a request for the Commission to require equipment manufacturers to, say, enter a new line of business, or to manufacture only large digital television sets based on the belief that programming looks better on a big screen, ancillary jurisdiction would not properly lie. But that is not the case.

\* \* \* \* \*

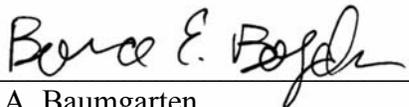
In *Southwestern Cable*, the Supreme Court gave credence to the Commission’s decision to take action to protect the integrity of terrestrial broadcast television based on the Commission’s belief that “we are in a critical period with respect to UHF development.” 392 U.S. at 176, n.44 (citation omitted). The issue under consideration in this proceeding comes at a similarly critical juncture for the industry. Absent action by the Commission to prevent the unauthorized retransmission of digital broadcast content, a new service that both Congress and the Commission have fostered – digital television – will founder. The Commission drove television broadcast stations to construct digital facilities at a pace unprecedented in the history of the rollout of new technologies on the theory that the availability of digital content would prompt consumers to acquire digital reception equipment. This theory, and the tremendous

financial and human resources that have been mobilized to advance it, require that digital broadcast stations have continued access to high quality digital content to deliver to consumers.

Respectfully submitted,

MOTION PICTURE ASSOCIATION OF AMERICA, INC.  
ABC  
ABC TELEVISION AFFILIATES ASSOCIATION  
AFMA  
AMERICAN ASSOCIATION OF ADVERTISING AGENCIES  
AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS  
AMERICAN SOCIETY OF COMPOSERS, AUTHORS AND PUBLISHERS  
ASSOCIATION FOR MAXIMUM SERVICE TELEVISION, INC.  
ASSOCIATION OF NATIONAL ADVERTISERS, INC.  
BELO CORP.

BROADCAST MUSIC, INC.  
CBS  
DIRECTORS GUILD OF AMERICA  
FOX BROADCASTING COMPANY  
INTERNATIONAL ALLIANCE OF THEATRICAL AND STAGE EMPLOYEES, MOTION PICTURE TECHNICIANS, ARTISTS AND ALLIED CRAFTS OF THE UNITED STATES, ITS TERRITORIES AND CANADA, AFL-CIO, CLC  
NATIONAL ASSOCIATION OF BROADCASTERS  
SCREEN ACTORS GUILD, INC.  
WRITERS GUILD OF AMERICA, EAST, INC.  
WRITERS GUILD OF AMERICA, WEST, INC.

By:   
Jon A. Baumgarten  
Bruce E. Boyden  
Proskauer Rose LLP  
1233 Twentieth Street NW, Suite 800  
Washington, DC 20034  
(202) 416-6800

Mace J. Rosenstein  
Jacqueline P. Cleary  
Hogan & Hartson LLP  
555 Thirteenth Street NW  
Washington, DC 20004  
(202) 637-5600

*Counsel for The Motion Picture Association of America, Inc.*

# **ATTACHMENT A**

# **White Paper**

*A Proposal for Protection of Unencrypted Digital Broadcast Television*

*December 6, 2002*

## **1 Summary of Conclusions**

1.1 The DTV transition promises new opportunities, but also poses new risks. The proposed implementation of the broadcast flag technology (the “Broadcast Flag Solution” or the “Solution”) set forth in the accompanying documents is a practical, economical solution to the problem of piracy of digital broadcast television content, one that is necessary in order to protect digital broadcast television content and facilitate a meaningful DTV transition, allowing its promise to be fulfilled.

1.2 The Broadcast Flag Solution is limited in scope: it is designed to prevent unauthorized redistribution only of digital broadcast television content outside the personal digital network environment, as defined below. The Solution does not prevent or limit the number of physical copies from being made within the home. It requires only that such copies be sufficiently secure so as to prevent such copies from being a source of unauthorized redistribution outside the home.

1.3 The Solution is narrowly tailored to apply directly only to products containing certain devices called “demodulators,” or other devices known as “modulators.” Other products would be required to protect digital broadcast content only in two very limited circumstances, and only if their manufacturers elected to receive such content. Furthermore, the Broadcast Flag Solution preserves manufacturer flexibility to the greatest extent possible. Manufacturers that choose to participate would have a wide range of expanding options of protection technologies to choose from in designing their products. The Solution also promotes the interests of consumers who wish to receive high-quality digital television content. And the Solution provides a fair, market-based procedure, administered by the FCC, for determining protection technologies authorized for use in regulated products (“Table A technologies”) that balances the interests of both content providers and manufacturers. Under this procedure, technologies may be authorized for use in protecting digital outputs or recording if it can be shown that they are already used or approved by content owners for the protection of valuable content, or if they are at least as effective as a technology that has already been authorized.

1.4 The outlines of the Broadcast Flag Solution have already received widespread, cross-industry support. This more specific proposal is put forward by the Motion Picture Association of America, Inc. (“MPAA”), ABC, ABC Television Affiliates Association, AFMA, American Association of Advertising Agencies (“AAAA”), American Federation of Television and Radio Artists (“AFTRA”), American Society of Composers, Authors and Publishers (“ASCAP”), Association for Maximum Service Television, Inc. (“MSTV”), Association of National Advertisers, Inc. (“ANA”), Belo Corp., Broadcast Music, Inc. (“BMI”), CBS, Directors Guild of America (“DGA”), Fox Broadcasting Company (“FBC”), International Alliance of Theatrical and Stage Employes, Motion Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada, AFL-CIO, CLC (“IATSE”), National Association of Broadcasters (“NAB”), Screen Actors Guild, Inc. (“SAG”), Writers Guild of America, East, Inc. (“WGA-East”), and Writers Guild of America, West, Inc. (“WGA-West”). In addition, the proposal is also supported by the Digital Transmission Licensing Administrator, LLC (commonly known as “5C”).

## **2      The Need for the Broadcast Flag Solution**

2.1      Unlike other digital programming distribution methods such as cable, satellite, or DVDs, digital broadcast television is transmitted in the clear, and thus is subject to an extraordinarily high risk of unauthorized redistribution. Once received in the home, digital broadcast television content can easily be redistributed via retransmission over networks like the Internet by such means as rebroadcasting, hosting files on a web server, or peer-to-peer file trafficking. Such unauthorized redistribution can be accomplished without downloading any special software, without the need for circumventing any copy protections, without such tools as analog-to-digital converters, or indeed without any complex technical skills whatsoever. For example, all a person has to do is to select “Record” while watching TV on his or her computer using a TV tuner card, and then save the file to a publicly accessible folder on his or her hard drive, where it can be illegally redistributed to anonymous users via peer-to-peer file trafficking. Or that person can easily e-mail the file as an attachment to an unlimited number of people. Or he or she can simply place the recorded file on a personal webpage for unauthorized redistribution to others on the Internet. The capability of the Internet to allow distribution worldwide, instantly, to millions of recipients, distinguishes the looming threat of digital piracy from previous technologies, such as the VCR, that rely on the creation and distribution of physical copies. With worldwide unauthorized redistribution of digital content so easy to accomplish, the threat of widespread piracy is enormous, even if the number of pirates is low. Any recipient of digital broadcast television, not just the professional pirate or amateur hacker, would have it within his or her power to illegally redistribute digital broadcast television content almost at will, everywhere on Earth.

2.2      Without a regulatory redistribution control regime such as the Broadcast Flag Solution, content providers are faced with the spectre of digital piracy on a massive scale of whatever content they make available for digital broadcast. Given the extent of such piracy, it would be impossible to combat the unauthorized retransmission of digital content effectively merely by pursuing individual infringement actions. Rather, a comprehensive regulatory framework must be established to ensure the protection of digital broadcast content as it enters consumer products. Otherwise, as broadcast television transitions into the digital era and as broadband capacity expands, we can expect that producers of compelling programming will recalculate their interest in licensing their most valuable content over a distribution mechanism so easily susceptible to unauthorized redistribution, and will consider instead limiting such programming to more secure channels such as conditional access systems. The DTV transition may, as a result, be seriously threatened.

2.3      A regulatory redistribution control regime is also necessary to preserve free consumer access to high-quality programming by means of broadcast television. Broadcast television is a unique resource, justly cherished by millions of Americans. The availability of compelling programming free of charge via broadcast television has been a staple of American culture since the 1950s. In addition to its importance domestically, broadcast television programming is a major United States export that is tremendously important both to the American economy and to our prestige in the world. For all of these reasons, broadcast television is a critically important resource that must be preserved.

2.4 High-value broadcast programming exists only because of the market foundation on which it has been built. A multi-billion dollar industry, employing thousands of individuals, broadcast television depends on an economic model that relies not on fees collected from the individual consumer, but on advertising revenue and on profits from resale rights both here and abroad. Under this model, broadcast television content providers have invested millions of dollars in producing expensive, high-quality, high-production-value programming. This programming could not exist without the expectation of the revenue generated by sales of advertisements in particular geographic markets and by syndication of programs after their initial broadcast. Content owners, directors, writers, actors, distributors, and others all depend on the existence of that revenue stream for their compensation and their ability to produce and distribute new works. Broadcast television programming has also contributed to the enormously important consumer electronics and computer industries. The wide availability of high-quality programming has driven increasing demand for these products.

2.5 The viability of the economic model upon which the broadcast television industry is built will be seriously undermined by rampant piracy if digital broadcast television content is not protected. Unauthorized redistribution would inflict enormous damage on both of the pillars upon which broadcast television now stands. It would cripple advertising revenue by hindering broadcast content providers' ability to distribute content on a territorial basis and to adapt advertising to particular markets; and it would seriously damage critically important resale and syndication rights.

2.6 The result could be the destruction of broadcast television programming as we currently know it. The loss of valuable programming via free, over-the-air broadcast television would reduce the rich range of options consumers presently have in choosing the means of viewing valuable content. Indeed, poorer consumers who may not be able to afford conditional access subscription fees may be shut out of obtaining quality television programming entirely, a consequence that would exacerbate fears of the emergence of a "two-tiered" information society.

### **3 Overview of the Broadcast Flag Solution**

#### **3.1 Scope of the Broadcast Flag Solution**

3.1.1 The Broadcast Flag Solution is designed to prevent unauthorized redistribution outside of the personal digital network environment. "Personal digital network environment" means the home or similar local environment. The "home" consists of all the rooms or areas within a consumer's primary residence. "Similar local environment" expands beyond the limited definition of "home" to include locations such as a consumer's car, boat, RV, or second home. "Personal digital network environment" thus covers any of these types of locations, but does not cover unauthorized or insecure transmission between or among them. That is, the Broadcast Flag Solution allows for a flexible definition of "personal digital network environment" to include electronic transmission of digital broadcast content between various locations typically associated with a consumer's home, but quite reasonably does not require content owners to accept unauthorized transmissions or intolerably low levels of security. Nor does the Broadcast Flag Solution itself limit a consumer's ability to make or move physical copies of broadcast content.

3.1.2 With respect to security, technologies to securely bind content to the personal digital network as it is being transferred between or among locations do not exist today. We invite and encourage the development of such technologies that could expand consumer choice so long as valuable rights in content are protected.

3.1.3 The Broadcast Flag Solution is not a form of broadcast copy protection. The Broadcast Flag Solution does not place restrictions on analog copying; for example, the Solution will have no impact on the use of VCRs. With respect to digital copying, the Solution allows the creation of digital recordings using authorized recording methods, and allows transmission between products using authorized digital outputs. Indeed, the technologies that MPAA member companies have thus far recognized as satisfying the criteria for Table A technologies — DTCP, HDCP, CPRM, and D-VHS — all allow secure digital transmission and recording within the personal digital network environment. We expect that future technologies will also satisfy the criteria in a similar manner.

## **3.2 Structure of the Broadcast Flag Solution**

3.2.1 The Broadcast Flag Solution begins when a digital broadcast television signal is demodulated -- that is, converted from a radio waveform to a digital data stream. Demodulation is where the risk of unauthorized redistribution commences; prior to demodulation, the digital broadcast television signal is in an unusable, modulated form. It is therefore critical that the content be required to be protected from the point of demodulation forward. The Broadcast Flag Solution achieves this by regulating all consumer products containing demodulators, requiring such products to handle digital broadcast content in a secure manner until it has been checked for the presence of the Broadcast Flag, and to pass the content only to certain other products that will handle it securely until it has been checked for the Flag.

3.2.2 In order for the Broadcast Flag Solution to be complete, products receiving a digital signal from a product containing a demodulation device must also protect against unauthorized redistribution. However, such products would become subject to the Requirements only in the case where their manufacturers opt, by making a written commitment to follow the Requirements, to make their products eligible in two limited situations to access digital broadcast television content in usable form.

3.2.3 The vast majority of products will be designed either not to access digital broadcast television content at all in usable form, or to access such content only after it has been passed from a regulated product via a protected output. Such products are not subject to the Requirements, although the latter products would be subject to any licensing terms imposed by the manufacturer of a Table A technology used to pass the content. In the case of a product receiving content over an analog output, or over a restricted DVI output, no requirements are imposed.

3.2.4 Consumer modulators are also regulated under the Solution. A “consumer modulator” is a device that converts a signal into the same form as is used by a digital broadcast television station. Such modulators can be used as a means of connecting products to a home network. However, if unregulated, consumer modulators could also be used to mislabel content that

originated in another protected distribution channel, such as view-only content distributed over a broadband connection or encrypted pay-per-view transmissions, as copyable digital television content. In other words, left unregulated, consumer modulators could be used as a “laundry channel.” In order to prevent such “Modulator Laundry Channels” from undermining other content protection systems, consumer modulators are required to refuse to pass content marked with the Broadcast Flag from “non-trusted sources.”

### **3.3 Description of the Broadcast Flag Solution**

3.3.1 Under the Broadcast Flag Solution, certain content may be embedded with the Broadcast Flag – the Redistribution Control descriptor set forth in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 2000, Amendment 3, 6 February 2002. The presence of the Flag means only that redistribution control is being asserted.

3.3.2 All consumer products containing demodulators, as well as certain other consumer products described above, must either check for the Flag, or protect the content as if it were marked with the Flag. If the Flag is found to be present, or if the content has not yet been screened, the product must protect the content from unauthorized redistribution under the Compliance and Robustness Requirements described below. If the Flag is not found to be present, the Requirements no longer apply.

3.3.3 Products specifically intended for professional and broadcast use are exempt from the Requirements. Retransmitters of DTV content in encrypted or unencrypted form, however, have additional obligations to ensure the protection of the content after retransmission.

## **4 Cost and Impact of the Broadcast Flag Solution**

4.1 Of the available alternatives, the Broadcast Flag Solution accomplishes the protection of digital broadcast content in the most economical and practical manner. Implementation of the Broadcast Flag Solution will bring digital television into an already existing framework of content protection. The Broadcast Flag itself is royalty free, and the Broadcast Flag Solution is easily implemented and an efficient solution for both the product manufacturer and the consumer.

4.2 The Broadcast Flag itself is merely a message in the ATSC stream that is fully compatible with current ATSC-compliant devices. The Broadcast Flag Solution will not prevent consumers’ existing equipment from displaying or recording content marked with the Flag. Since analog outputs are a permitted output under the Requirements, existing analog displays, players, and recorders will continue to function with the new compliant products under the Compliance and Robustness Requirements. Furthermore, the restrictions imposed by the Broadcast Flag Solution on digital outputs will hardly be unusual considering existing private contractual agreements for the protection of conditional access television and other forms of content. Enactment of the Broadcast Flag Solution will ensure that digital broadcast television is protected in a similar fashion as with every other form of digital audiovisual content, but without the limitations on copying that other protection arrangements may impose. Moreover, secure

copies will be viewable on the playback facility of the recorder that made them. Thus, any incidental incompatibility between secure recordings and legacy players will commonly involve distribution of the recording to other persons or locations. In order to achieve a balanced solution, however, this incidental legacy issue must not be used to undermine needed security of freely permitted copies.

4.3 As noted, the Broadcast Flag will in no way retard the development of new consumer technologies. Under the criteria for Table A, any technology that has achieved marketplace acceptance, or that is at least as effective as a technology already on Table A, can be added to Table as an authorized technology. We envision that Table A will grow to include a diverse population of authorized technologies as competing technology manufacturers vie to capture more market share. Four such technologies have already gained sufficient industry acceptance to qualify as authorized technologies, while several others are in development that have the potential to be equally effective.

4.4 Similarly, the Broadcast Flag Solution will not, in itself, interfere in any way with continued innovation in the development of open source software. While building a secure open source protection technology will no doubt be a challenge, it is a challenge faced by open source programmers in developing *any* secure application, not just Table A technologies. We welcome the efforts of open source programmers to meet this challenge and develop secure digital output protection technologies and recording methods for submission for inclusion on Table A.

4.5 The cost impact on affected products of implementing the Broadcast Flag Solution will be insignificant. Already, several technologies worthy of listing on Table A exist in the marketplace, even without the Broadcast Flag Solution, thus proving that such technologies are both affordable and readily available. The vast majority of products will also record, process, and display pay television and other types of content that will require such technologies be implemented even without the Broadcast Flag Solution. In addition, many products are already manufactured under private licensing arrangements that are very similar to the Compliance and Robustness Requirements. The existence of such products is additional proof that the cost impact of the Broadcast Flag Solution will be negligible.

## **5 The Compliance and Robustness Requirements**

5.1 The Compliance and Robustness Requirements are the heart of the Broadcast Flag Solution. Together, these Requirements ensure both that digital broadcast television content is protected within regulated products, and that it cannot be transferred to a location that is insecure.

5.2 The Compliance Requirements restrict the types of outputs and recording methods that may be employed by regulated products. Under the Compliance Requirements, digital outputs and recording methods must be protected by one or more authorized technologies to prevent unauthorized redistribution. In limited cases, digital outputs and recording methods may be protected by a self-certified Robust Method, where the content has been neither screened nor processed after demodulation or where the content is passed in a certain way within a computer.

5.3 The Robustness Requirements require products to be secure against attempts to access protected content. The Robustness Requirements include the requirement, included in similar content protection technology agreements, that source products and Downstream Products “shall be manufactured in a manner clearly designed to effectively frustrate” attempts to modify such products to defeat the Compliance Requirements. Under the Robustness Requirements, products must meet a specified level of secure design and construction, for example, by employing encryption techniques and being tamper-resistant.

5.4 An additional requirement is necessary in order to prevent another form of the “laundry channel” problem – what might be called the Unscreened Content Laundry Channel. Under the Requirements, a product containing a demodulation device may output or record digital broadcast television content without screening the content first. Such “Unscreened Content” must be treated as if it contains the Flag, until it is screened. However, while the Requirements define “Unscreened Content” as digital broadcast television content, which is copyable, a product receiving such “Unscreened Content” has no way of determining whether the content is copyable broadcast television content or “Copy Never” content taken from elsewhere until the content is examined. If unexamined content is allowed to leave a compliant product via a Table A technology with no obligations to check for the Flag, such products could be used to mislabel content that originated in another protected distribution channel, such as view-only content distributed over a broadband connection or encrypted pay-per-view transmissions, as copyable digital television content. In order to prevent the creation of such an “Unscreened Content Laundry Channel,” the Requirements provide that Table A technologies must check for the Flag, or require other products to do so.

## **6 Authorized Output and Recording Protection Technologies**

6.1 One of the key components of the Broadcast Flag Solution is the provision that consumer electronics and computer manufacturers in most instances be required to use one or more of the Table A technologies in designing the digital outputs and recording methods of their products. Without such a requirement, there would be no guidance to product manufacturers as to what technologies to include, insufficient certainty concerning the standards to be met, and unavoidable contention between content providers and manufacturers concerning the meaning of the Requirements. Such an environment would be antithetical to the DTV transition, and would necessarily involve the FCC in constant adjudicatory actions.

6.2 The solution to this problem is to specify particular authorized output and recording protection technologies that regulated products may use. Instead of locking in technological mandates that may quickly become obsolete, or abstract concepts that offer little guidance, the Solution adopts a flexible, market-based approach under which a technology is authorized for Table A if it has been accepted in the relevant marketplace as a protection technology or is just as effective as one that has. The Broadcast Flag Solution contains fair and carefully balanced procedures for continually adding new technologies to the list. This method of protecting outputs and recordings ensures that innovation in the product manufacturing industry continues unabated. Continued innovation not only benefits technology manufacturers and consumers, but also content providers, who will benefit most of all from the creation of a continually evolving list of state-of-the-art technologies for content protection.

6.3 The Broadcast Flag Solution includes several procedures to determine if a technology has been accepted in the marketplace. If a technology provider believes its technology meets one of the criteria, it may file an application stating the grounds for its belief. The companies named in the application as having “used or approved” the technology in the market would then be requested to respond; if the companies do not respond to the request, they will be deemed to have admitted the facts alleged in the application. Any remaining dispute would be fairly but swiftly resolved by Commission staff.

6.4 While appropriately respectful of marketplace decisions, the Broadcast Flag Solution also includes a safeguard provision under which Commission staff may determine that the marketplace has been unreasonably slow in adopting a proposed technology that is just as effective as a technology already on Table A. The safeguard provision is intended to address any concerns about the fairness of market-based criteria. Indeed, the procedures for this safeguard provision are more detailed than any other procedure contained in the Broadcast Flag Solution. Under the safeguard provision, the proponent of a new technology that is “at least as effective” as a technology already on Table A may apply to have it added to the list. The Commission will issue a public notice providing 60 days for comment on the request to place the technology on Table A. In reaching its decision, the Commission staff will consider not only the effectiveness of the proposed technology in protecting digital television content from unauthorized redistribution, but also any applicable license terms of the technology relating to security, enforcement, and updates.

6.5 Although the proposed regulations do not identify particular technologies that should be added to Table A upon enactment, it is important that the Commission act immediately upon issuing these regulations to simultaneously identify appropriate technologies to be admitted to Table A. Swift approval of an initial set of technologies is necessary to facilitate the digital television roll-out, to protect digital broadcast television content as soon as the regulations become effective, and to inform manufacturers of the technical means of implementing the Broadcast Flag Solution.

6.6 The Broadcast Flag Solution recognizes that some Table A technologies may be compromised. Therefore, to protect against inevitable hacks, the Solution includes a procedure by which a request can be made to remove a technology from Table A if it has been compromised. The Commission would make a timely determination as to whether or not such technology should be removed from Table A. In doing so, the Commission would consider two factors: the protection of digital television against unauthorized redistribution, and the impact on content owners, consumers and manufacturers resulting from the continued use of the compromised technology and from any removal of the technology from the list.

## **7 Digital Broadcast Television Retransmitted by Cable and Satellite Systems**

7.1 The Requirements apply only to “Unencrypted Digital Terrestrial Broadcast Content” -- content broadcast “without encrypting or otherwise making the content available through a technical means of conditional access.” However, digital broadcast content should also be protected when retransmitted by cable or satellite systems. In the case of unencrypted cable

retransmission, the Requirements take hold upon demodulation by the consumer's set-top box, the same as DTV demodulation. Other retransmitters, however, such as direct broadcast satellite systems, not only use a variety of changing modulation methods not readily specified in the Requirements, but also encrypt retransmitted broadcast television signals, making it impossible to check such signals for the Flag until they are decrypted. In order to ensure that retransmitted digital broadcast television content is protected, the Requirements provide that retransmitters that encrypt digital broadcast television signals must either check for the Flag themselves at the head end or require the set-top box to check for the Flag on decryption of the signal. If the Flag is present, the retransmitter must require the consumer set-top box or other receiving product to abide by the Requirements as if it contained a covered demodulation function.

## **8 Effective Date**

8.1 Consistent with industry practice, some period of time must be given before manufacturers must cease manufacturing and distributing products that are not in compliance with the Compliance and Robustness Requirements. Given the low cost and the technical ease of implementing the Broadcast Flag Solution, and the fact that no licenses will need to be negotiated to use the Flag, twelve months is a sufficient amount of lead time following adoption of the Requirements by the Commission.

[END]

# **ATTACHMENT B**

**Requirements for the Protection of  
Unencrypted Digital Terrestrial Broadcast Content  
Against Unauthorized Redistribution**

**Joint Proposal from MPAA and 5C Companies  
December 6, 2002**

**Scope**

This document sets forth requirements to be imposed on certain products that demodulate unencrypted digital terrestrial broadcast content and certain other products that modulate content which could be sent to demodulators, in order to protect unencrypted digital terrestrial broadcast content against unauthorized redistribution (including unauthorized redistribution over the Internet), without permitting content whose provenance is unknown from being treated as unencrypted digital terrestrial broadcast content.

**[X.] Requirements.**

**X.1 Definitions.**

“8-VSB” means vestigial sideband modulation with 8 discrete amplitude levels, as described in ATSC Standard A/53.

“16-VSB” means vestigial sideband modulation with 16 discrete amplitude levels, as described in ATSC Standard A/53.

“64-QAM” means Quadrature Amplitude Modulation with a 64-point constellation, as described in “Digital Video Transmission Standard for Cable Television”, ANSI/SCTE 07 2000.

“256-QAM” means Quadrature Amplitude Modulation with a 256-point constellation, as described in “Digital Video Transmission Standard for Cable Television”, ANSI/SCTE 07 2000.

“Authorized Digital Output Protection Technology” means a technology listed on Table A, as such list may be amended from time to time pursuant to [regulations to be promulgated by the Commission concerning the authorization of digital output technologies].

“Authorized Recording Method” means a recording method listed on Table A, as such list may be amended from time to time pursuant to [regulations to be promulgated by the Commission concerning the authorization of recording technologies].

“Bona Fide Reseller” means a person regularly engaged, or about to become regularly engaged, in the lawful commercial enterprise of selling, reselling, manufacturing, or assembling Modulation Functions or Demodulation Functions, or products incorporating Modulation Functions or Demodulation Functions, in compliance with this subpart.

“Broadcast Flag” means the Redistribution Control descriptor (rc\_descriptor()) described in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 2000, Amendment 3, 6 February 2002.

“Circumvention Devices” means devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this Section X.

“Computer Product” means a product that is designed for or permits the end user to install a wide variety of commercially available software applications thereon, such as a personal computer, handheld “Personal Digital Assistant” and the like, and further includes a subsystem of such a product, such as a graphics card.

“Covered Demodulator Product” means a product (whether a physical device, software or combination thereof) that is required under Sections X.2(a)(1) or X.2(b)(1) to comply with the Demodulator Compliance Requirements, and to be manufactured in accordance with the Demodulator Robustness Requirements.

“Covered Modulator Product” means a product (whether a physical device, software or combination thereof) that is required under Section X.13(a)(1) to comply with the Modulator Compliance Requirements, and to be manufactured in accordance with the Modulator Robustness Requirements.

“Demodulation Function” means a component, or set of components, that is designed to perform the function of 8-VSB, 16-VSB, 64-QAM or 256-QAM demodulation and thereby produce a data stream consistent with ATSC Standard A/53 Annex C (e.g., a demodulation chip or demodulation software).

“Demodulator Compliance Requirements” means the requirements set out in Sections X.3 through X.6.

“Demodulator Robustness Requirements” means the requirements set out in Sections X.7 through X.12.

“Downstream Product” means a product (whether a physical device, software or combination thereof) that is capable of accessing in usable form<sup>1</sup> Unscreened Content or Marked Content<sup>2</sup> passed to such product via a Robust Method, where the manufacturer of such product has committed in writing in accordance with Section X.2(c) that such product will comply with the Demodulator Compliance Requirements and be manufactured in accordance with the Demodulator Robustness Requirements, such that such product shall be a Covered Demodulator Product.<sup>3</sup>

“EIT” means Event Information Table as defined in ATSC Standard A/65A (2000) Program and System Information Protocol for Terrestrial Broadcast and Cable.

“Hardware” means a physical device, including a component, that implements in a Covered Demodulator Product or Covered Modulator Product, as applicable, any of the content protection requirements set forth in the respective Demodulator Compliance Requirements or Modulator Compliance Requirements and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such product or (ii) includes instructions or data that are not permanently embedded in such product where such instructions or data have been customized for such product and such instructions or data are not accessible to the end user through the product.

“Marked Content” means, with respect to a Covered Demodulator Product, Unencrypted Digital Terrestrial Broadcast Content that such product has (a) received and demodulated using its Demodulation Function and for which such product has inspected either the EIT or PMT and determined the Broadcast Flag to be present or (b) where such product is a Downstream Product, received via a Robust Method<sup>4</sup> and accessed in usable form, and for which such product either inspected the EIT or PMT and determined the Broadcast Flag to be present or determined through information robustly conveyed with such content (via such Robust Method) that another Covered Demodulator Product had previously so screened such content and determined the Broadcast Flag to be present; provided, however, that, with respect to a Covered Demodulator Product, “Marked

---

<sup>1</sup> The fact that a stream containing Unscreened Content or Marked Content has not been altered following demodulation does not mean in and of itself that such content is not in “usable form”.

<sup>2</sup> Note that it is only pursuant to Section X.6(a) that Marked Content may be passed from a Covered Demodulator Product using a Robust Method.

<sup>3</sup> Note that Downstream Products would be required under Section X.2 to comply with the Demodulator Compliance Requirements and Demodulator Robustness Requirements prior to being sold or distributed (i.e., a failure to comply with such requirements would be a violation of, and subject to enforcement by the Commission under, this subpart).

<sup>4</sup> See note 2 above.

Content” shall not include content that has been passed from such product pursuant to Section X.4(a)(1), X.4(a)(2), X.4(a)(3), X.4(a)(5), X.4(a)(6), or X.6(b).<sup>5</sup>

“Modulation Function” means a component, or set of components, that is designed to perform the function of generating and emitting 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated signals (e.g., a modulation chip or modulation software).

“Modulator Compliance Requirements” means the requirements set out in Section X.14.

“Modulator Robustness Requirements” means the requirements set out in Sections X.15 through X.18.

“PMT” means Program Map Table as defined in ISO/IEC IS 13818-1:1 2000 (E), International Standard, MPEG-2 Systems.

“Robust Method” means, with respect to the passing of Unscreened Content or Marked Content from one product to another, a method that complies with Section X.10.

“Software” means the implementation in a Covered Demodulator Product or a Covered Modulator Product, as applicable, of any of the content protection requirements set forth in the respective Demodulator Compliance Requirements or Modulator Compliance Requirements through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware.

“Transitory Image” means data that has been stored temporarily for the sole purpose of enabling a function not prohibited by this Section X but that (a) does not persist materially after such function has been performed and (b) is not stored in a way that permits copying or storing of such data for other purposes.

“Unencrypted Digital Terrestrial Broadcast Content” means audiovisual content contained in the ATSC Transport Stream broadcast by a digital television station in compliance with the digital broadcast television transmission standard set forth in 47 C.F.R. Section 73.682(d), without encrypting or otherwise making the content available through a technical means of conditional access, and includes such content when retransmitted in unencrypted digital form.

“Unknown Content” means, with respect to a Covered Modulator Product, any audiovisual content that such product has received in unencrypted form, other than

---

<sup>5</sup> Note: The fact that content *passed from* a Covered Demodulator Product pursuant to Sections X.4(a)(2) and X.4(a)(5) is not Marked Content with respect to that product does not remove any obligation on the part of Covered Demodulator Products that *receive* such content to treat such content as Marked Content.

audiovisual content that such product has received and demodulated using a Demodulation Function or that has been passed from such Covered Modulator Product.

“Unscreened Content” means, with respect to a Covered Demodulator Product, Unencrypted Digital Terrestrial Broadcast Content that such product either (a) received and demodulated using its Demodulation Function and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag or (b) where such product is a Downstream Product, received via a Robust Method and accessed in usable form, and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag and has not determined through information robustly conveyed with such content (via such Robust Method) that another Covered Demodulator Product had previously so screened such content and determined the Broadcast Flag to be present; provided, however, that, with respect to a Covered Demodulator Product, “Unscreened Content” shall not include content that has been passed from such product pursuant to Sections X.3(a)(1), X.3(a)(2), X.3(a)(3), X.3(a)(4), X.3(a)(6), X.3(a)(7), or X.6(b).<sup>6</sup>

“User 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. A “User Accessible Bus” does not include memory buses, CPU buses, or similar portions of a device’s internal architecture that do not permit access to content in a form usable by end users.

## **X.2 Sale or Distribution of Demodulation Functions and Downstream Products.**

### **(a) Demodulation Functions.**

(1) No person<sup>7</sup> that manufactures in the United States or imports from any foreign country into the United States, a Demodulation Function shall sell or distribute in interstate commerce such Demodulation Function unless:

(A) at the time of such sale or distribution such Demodulation Function is, or is incorporated into, a product that complies with the Demodulator Compliance Requirements and was manufactured in accordance with the Demodulator Robustness Requirements; or

---

<sup>6</sup> Note: The fact that content *passed from* a Covered Demodulator Product pursuant to Sections X.3(a)(2), X.3(a)(4), and X.3(a)(6) is not Unscreened Content with respect to that product does not remove any obligation on the part of Covered Demodulator Products that *receive* such content to treat such content as Unscreened Content.

<sup>7</sup> “Person” shall be defined as in 47 U.S.C. § 153(32).

(B) such sale or distribution is to a person that has committed in writing pursuant to Section X.2(c) not to sell or distribute such Demodulation Function in the United States other than in accordance with Sections X.2(a)(1)(A) or X.2(a)(1)(B).

(2) No person shall manufacture in the United States, or import from any foreign country into the United States, a Demodulation Function for the purpose of sale or distribution in interstate commerce other than sale or distribution in interstate commerce in accordance with Sections X.2(a)(1)(A) or X.2(a)(1)(B).

(3) No person shall sell or distribute in interstate commerce a Covered Demodulator Product if: (A) the person has actual knowledge that the Covered Demodulator Product does not comply with the Demodulator Compliance Requirements and Demodulator Robustness Requirements; (B) the Covered Demodulator Product has been determined by the Commission or a court of competent jurisdiction not to comply with the Demodulator Compliance Requirements and Demodulator Robustness Requirements; or (C) the person has failed to expeditiously disclose to the Commission, upon request by the Commission, information that person may have in its possession identifying the source of the product in question.

(4) Paragraph X.2(a)(3) shall not apply to an individual person for the resale of a product that was manufactured prior to the effective date of this subpart or that initially was sold or distributed in compliance with this subpart.

**(b) Downstream Products.**

(1) No person shall manufacture in the United States, sell or distribute in interstate commerce, or import from any foreign country into the United States a Downstream Product unless, at the time of such manufacture, sale, distribution, or importation, such Downstream Product complies with the Compliance Requirements and was manufactured in accordance with the Robustness Requirements.

(2) Paragraph X.2(b)(1) shall not apply to an individual person for the resale of a Downstream Product that was manufactured prior to the effective date of this subpart or that initially was sold or distributed in compliance with this subpart.

**(c) Written Commitments.**

(1) A commitment in writing for a Downstream Product or to allow sale or distribution under Section X.2(a)(1)(B) shall be filed on a form prescribed by the Commission. The commitment shall be signed as provided in \_\_\_ and submitted to the Federal Communications Commission, [address].

(2) Among the information to be provided by a person filing a commitment in writing pursuant to this Section X.2(c) for a Downstream Product shall be a commitment that that the person is engaged, or about to become engaged, in the lawful commercial enterprise of manufacturing such Downstream Product, and that such product will comply with the Demodulator Compliance Requirements and be manufactured in accordance with the Demodulator Robustness Requirements.

(3) Among the information to be provided by a person filing a commitment in writing pursuant to this Section X.2(c) to allow sale or distribution under Section X.2(a)(1)(B) shall be a commitment that one of the following conditions is true:

(A) the person is a Bona Fide Reseller;

(B) the person is a licensed digital television broadcaster; or

(C) the person is a satellite broadcaster, cable television system operator, or other person engaged, or about to become engaged, in the lawful retransmission of Unencrypted Digital Terrestrial Broadcast Content pursuant to Section X.2(d) or X.2(e).

(4) It shall be a violation of this subpart for a person to sell or distribute a Demodulation Function pursuant to Section X.2(a)(1)(B) to any person that the person knows, or reasonably should know, does not meet any of the conditions set forth in Section X.2(c)(3).

(5) It shall be a violation of this subpart, enforceable by the Commission, for any person that has filed a written commitment pursuant to this Section X.2(c) to (A) in the case of such commitment under X.2(a)(1)(B), sell or distribute the Demodulation Function in the United States other than in accordance with Sections X.2(a)(1)(A) or X.2(a)(1)(B); or (B) in the case of such commitment for a Downstream Product, manufacture in the United States, sell or distribute in interstate commerce, or import from any foreign country into the United States the Downstream Product other than in compliance with Section X.2(b). To the extent that the filing of a written commitment pursuant to this Section X.2(c) creates rights between parties that may be enforced through private contractual remedies or third-party beneficiary rights, enforcement by the Commission will not abrogate those rights and remedies.

(6) The filing of a written commitment will be publicly announced in a timely manner by the Commission, and shall be available in accordance with Secs. 0.441 through 0.470 of this chapter.

**(d) Encrypted Retransmission.** Where a satellite broadcaster, cable television system operator, or any other person retransmits Unencrypted Digital Terrestrial Broadcast

Content in encrypted form, such retransmitter shall, upon demodulation of the 8-VSB, 16-VSB, 64-QAM or 256-QAM signal, inspect either the EIT or PMT for the Broadcast Flag, and if the Broadcast Flag is present (1) securely and robustly convey that information to the consumer product used to decrypt the retransmitter's signal information and (2) require that such consumer product, following such decryption, protect the content of such signal as if it were a Covered Demodulator Product receiving Marked Content.

**(e) Unencrypted Retransmission.** Where a satellite broadcaster, cable television system operator, or any other person retransmits Unencrypted Digital Terrestrial Broadcast Content in unencrypted form, such retransmitter shall, upon demodulation: (1) preserve the Broadcast Flag, if present, in both the EIT and PMT; and (2) use 8-VSB, 16-VSB, 64-QAM, or 256-QAM signal modulation for the retransmission.

### **X.3 Compliance Requirements for Covered Demodulator Products: Unscreened Content.<sup>8</sup>**

**(a)** A Covered Demodulator Product shall not pass, or direct to be passed, Unscreened Content to any output except

- (1) to an analog output;
- (2) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that such Covered Demodulator Product is compliant with Section X.14;
- (3) to a digital output protected by an Authorized Digital Output Protection Technology that is authorized for use with Unscreened Content pursuant to Section X.19, in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology;
- (4) where the stream containing such content has not been altered following demodulation and such Covered Demodulator Product outputs, or directs to be output, such content to a Downstream Product solely within the home or other, similar local environment, using a Robust Method;
- (5) where such Covered Demodulator Product outputs, or directs to be output, such content to another product and such Covered Demodulator Product exercises sole control (such as by using a cryptographic protocol), in compliance with the

---

<sup>8</sup> No requirements or limitations are imposed by this Section X with respect to the output, recording, or other handling of content other than Unscreened Content, Marked Content, and Unknown Content.

Demodulator Robustness Requirements, over the access to such content in usable form in such other product;

(6) where such Covered Demodulator Product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to Section X.3(b)(2), where such content is protected by the corresponding recording method<sup>9</sup>; or

(7) where such Covered Demodulator Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than (a) 350,000 pixels per frame (e.g. an image with resolution of 720 x 480 pixels for a 4:3 (non-square pixel) aspect ratio) and (b) 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

**(b)** A Covered Demodulator Product shall not record or cause the recording of Unscreened Content in digital form unless such recording is made using one of the following methods:

(1) a method that effectively and uniquely associates such recording with a single Covered Demodulator Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under this Section X; or

(2) an Authorized Recording Method that is authorized for use with Unscreened Content pursuant to Section X.19, in accordance with any obligations set out in Table A applicable to such Authorized Recording Method (provided that for recordings made on removable media, only Authorized Recording Methods expressly identified on Table A for use in connection with removable media may be used).

This Section X.3(b) does not impose restrictions regarding the storage of Unscreened Content as a Transitory Image.

---

<sup>9</sup> For example, a protected recording made onto storage media located in an external drive, where the recorder first encrypts the content and then passes it to the drive via an output.

#### **X.4 Compliance Requirements for Covered Demodulator Products: Marked Content.**

**(a)** A Covered Demodulator Product shall not pass, or direct to be passed, Marked Content to any output except

(1) to an analog output;

(2) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that such Covered Demodulator Product is compliant with Section X.14;

(3) to a digital output protected by an Authorized Digital Output Protection Technology, in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology;

(4) where such Covered Demodulator Product outputs, or directs to be output, such content to another product and such Covered Demodulator Product exercises sole control (such as by using a cryptographic protocol), in compliance with the Demodulator Robustness Requirements, over the access to such content in usable form in such other product;

(5) where such Covered Demodulator Product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to Section X.4(b)(2), where such content is protected by the corresponding recording method<sup>10</sup>; or

(6) where such Covered Demodulator Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than (a) 350,000 pixels per frame (e.g., an image with resolution of 720 x 480 pixels for a 4:3 (non-square pixel) aspect ratio) and (b) 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

---

<sup>10</sup> For example, a protected recording made onto storage media located in an external drive, where the recorder first encrypts the content and then passes it to the drive via an output.

**(b)** A Covered Demodulator Product shall not record or cause the recording of Marked Content in digital form unless such recording is made using one of the following methods:

(1) a method that effectively and uniquely associates such recording with a single Covered Demodulator Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under this Section X or

(2) an Authorized Recording Method, in accordance with any obligations set out in Table A applicable to such Authorized Recording Method (provided that for recordings made on removable media, only Authorized Recording Methods expressly identified on Table A for use in connection with removable media may be used).

This Section X.4(b) does not impose restrictions regarding the storage of Marked Content as a Transitory Image.

**X.5 Compliance Requirements for Covered Demodulator Products: Audio.** Except as otherwise provided in Sections X.3(a) or X.4(a), Covered Demodulator Products shall not output the audio portions of Unscreened Content or of Marked Content in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits.

**X.6 Add-in Covered Demodulator Products.**<sup>11</sup> Where a Covered Demodulator Product passes Unscreened Content or Marked Content from such Covered Demodulator Product to another product, other than where such Covered Demodulator Product passes, or directs to be passed, such content to an output (e.g., where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer), it shall so pass such content (a) using a Robust Method; or (b) protected by an Authorized Digital Output Protection Technology (which, in the case of Unscreened Content, is authorized for use with Unscreened Content pursuant to Section X.19), in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology. Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.

---

<sup>11</sup> This section does not generally incorporate Downstream Products into Section X.4(a) or override the limitations of Section X.3(a)(4).

## **X.7 Robustness Requirements for Covered Demodulator Products: Construction.**

(a) Covered Demodulator Products shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such products to defeat the Demodulator Compliance Requirements.

(b) Covered Demodulator Products shall not include:

- (1) switches, buttons, jumpers or software equivalents thereof,
- (2) specific traces that can be cut, or
- (3) functions (including service menus and remote-control functions),

in each case by which the Demodulator Compliance Requirements can be defeated, or by which compressed unencrypted Marked Content or compressed unencrypted Unscreened Content in such Covered Demodulator Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Section X.<sup>12,13</sup>

(c) Covered Demodulator Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal any secret keys or secret algorithms used to meet the requirements set forth in the Demodulator Compliance Requirements.

## **X.8 Robustness Requirements for Covered Demodulator Products: Data Paths.**

Within a Covered Demodulator Product, neither Unscreened Content nor Marked Content shall be present on any User Accessible Bus in unencrypted, compressed form.

(a) **Uncompressed Content.** During a petition opportunity that the Commission may designate, an interested person may petition the Commission to initiate a Notice of Inquiry to determine whether it is technically feasible and commercially reasonable to require that Unscreened Content and Marked Content when transmitted over any User Accessible Bus in uncompressed digital form be made reasonably secure from unauthorized interception by using means that meet the standards set forth in Section X.11. Such petition shall include evidence that such an inquiry is warranted in light of generally available technologies and existing commercial circumstances. Should the

---

<sup>12</sup> See Section X.8(a). It is anticipated that if the Demodulator Robustness Requirements are modified in the future to require protection of uncompressed data on a User Accessible Bus, the requirements of Section X.7(b) would also then be modified to apply to uncompressed unencrypted content.

<sup>13</sup> For avoidance of doubt, the provisions of Section X.7(b) prohibit inclusion of such means by which such defeating or exposure can occur through removal of the Broadcast Flag.

Commission, based on such evidence and on consultation with affected industries, proceed with such Notice of Inquiry and thereby determine that requiring such protection at such level is technically feasible and commercially reasonable, the Commission may, pursuant to a Notice of Proposed Rulemaking, revise these Demodulator Robustness Requirements to so require. The Commission will consider in its analysis: the general availability of relevant technologies, cost of implementation, effectiveness of any solutions, availability of alternative solutions, intellectual property licensing issues, consistency with requirements of other content protection systems, likely ability of manufacturers of Covered Demodulator Products to satisfy the Demodulator Robustness Requirements, and normal design cycles for such products. The Commission will exercise its discretion to limit the frequency of such Notices of Proposed Rulemaking.

### **X.9 Methods of Making Functions in Covered Demodulator Products Robust.**

Covered Demodulator Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

**(a) Distributed Functions.** Where compressed Unscreened Content or compressed Marked Content is delivered from one portion of the Covered Demodulator Product to another portion of such Covered Demodulator Product, whether among integrated circuits, software modules, a combination thereof, or otherwise, such portions shall be designed and manufactured in a manner associated and otherwise integrated with each other such that such Unscreened Content or Marked Content, as the case may be, in any usable form flowing between such portions of such Covered Demodulator Product shall be reasonably secure from being intercepted or copied except as permitted under the Demodulator Compliance Requirements.

**(b) Software.** Without limiting the requirements of Sections X.7 and X.8, portions of a Covered Demodulator Product that implement in Software the content protection requirements set forth in the Demodulator Compliance Requirements shall:

- (1) Comply with Section X.7(c) by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode (i.e. in kernel mode), and/or embodiment in a secure physical implementation; and, in addition, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.
- (2) Be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide access to unencrypted Unscreened Content or unencrypted Marked Content. For purposes of this Section X.9(b)(2), a “modification” includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections X.7 and X.8. This

Section X.9(b)(2) requires at a minimum the use of signed code or more robust means of “tagging” operating throughout the code. For purposes of this Section X.9(b), “signed code” means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as effective, to form a digital signature over Software such that its authenticity and integrity can be verified.

**(c) Hardware.** Without limiting the requirements of Sections X.7 and X.8, the portions of a Covered Demodulator Product that implement in Hardware the content protection requirements set forth in the Demodulator Compliance Requirements shall:

(1) Comply with Section X.7(c) by any reasonable method including but not limited to (x) embedding any secret keys or secret cryptographic algorithms used to meet the content protection requirements set forth in the Demodulator Compliance Requirements in silicon circuitry or firmware that cannot reasonably be read or (y) employing the techniques described above for Software.

(2) Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements set forth in the Demodulator Compliance Requirements in Covered Demodulator Products would pose a serious risk of rendering the Covered Demodulator Product unable to receive, demodulate, or decode Unencrypted Digital Terrestrial Broadcast Content. By way of example, a component that is soldered rather than socketed, or affixed with epoxy, may be appropriate for this means.

**(d) Hybrid.** The interfaces between Hardware and Software portions of a Covered Demodulator Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection that would be provided by a pure Software implementation.

**X.10 Robustness Requirements for Covered Demodulator Products: Robust Methods.** Where a Covered Demodulator Product passes, or directs to be passed, Unscreened Content or Marked Content from such Covered Demodulator Product to another product pursuant to Section X.6(a), it shall do so using a method designed to ensure that such content, in any usable form, shall be reasonably secure from being intercepted, redistributed or copied when being so passed to such other product. Where a Covered Demodulator Product passes, or directs to be passed, Unscreened Content to an output pursuant to Section X.3(a)(4), it shall do so using a method that provides technological protection against unauthorized redistribution of such content that is at least as effective as such technological protection provided by any one of the Authorized Digital Output Protection Technologies and that is designed to ensure that such content

may be accessed in usable form by another product only if such other product is a Downstream Product.

**X.11 Robustness Requirements for Covered Demodulator Products: Level of Protection.** The content protection requirements set forth in the Demodulator Compliance Requirements and the requirements set forth in Sections X.7(c) and X.8 shall be implemented in a reasonable method so that they:

(a) Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons, or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers, other than Circumvention Devices; and

(b) Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section X.11(a) such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

**X.12 Robustness Requirements for Covered Demodulator Products: Advance of Technology.** Although an implementation of a Covered Demodulator Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Covered Demodulator Product, would have caused such products to fail to comply with these Demodulator Robustness Requirements (“New Circumstances”). If a manufacturer of a Covered Demodulator Product has actual notice or actual knowledge of New Circumstances that relate to the manufacturer’s specific implementation of a Covered Demodulator Product (hereinafter referred to as “Notice”), then within 18 months after Notice such manufacturer shall cease distribution of such Covered Demodulator Product and shall only distribute Covered Demodulator Products that are compliant with the Demodulator Robustness Requirements in view of the then-current circumstances.

**X.13 Sale or Distribution of Modulation Functions.**

(a) **Modulation Functions.**

(1) No person<sup>14</sup> that manufactures in the United States or imports from any foreign country into the United States, a Modulation Function shall sell or distribute in interstate commerce such Modulation Function unless:

(A) at the time of such sale or distribution such Modulation Function is, or is incorporated into, a product that complies with the Modulator Compliance Requirements and was manufactured in accordance with the Modulator Robustness Requirements; or

(B) such sale or distribution is to a person that has committed in writing pursuant to Section X.13(b) not to sell or distribute such Modulation Function in the United States other than in accordance with Sections X.13(a)(1)(A) or X.13(a)(1)(B).

(2) No person shall manufacture in the United States, or import from any foreign country into the United States, a Modulation Function for the purpose of sale or distribution in interstate commerce other than sale or distribution in interstate commerce in accordance with Sections X.13(a)(1)(A) or X.13(a)(1)(B).

(3) No person shall sell or distribute in interstate commerce a Covered Modulator Product if: (A) the person has actual knowledge that the Covered Modulator Product does not comply with the Modulator Compliance Requirements and Modulator Robustness Requirements; (B) the Covered Modulator Product has been determined by the Commission or a court of competent jurisdiction not to comply with the Modulator Compliance Requirements and Modulator Robustness Requirements; or (C) the person has failed to expeditiously disclose to the Commission, upon request by the Commission, information that person may have in its possession identifying the source of the product in question.

(4) Section X.13(a)(3) shall not apply to an individual person for the resale of a product that was manufactured prior to the effective date of this subpart or that initially was sold or distributed in compliance with this subpart.

**(b) Written Commitments.**

(1) A commitment in writing to allow sale or distribution under Section X.13(a)(1)(B) shall be filed on a form prescribed by the Commission. The commitment shall be signed as provided in \_\_\_\_ and submitted to the Federal Communications Commission, [address].

---

<sup>14</sup> “Person” shall be defined as in 47 U.S.C. § 153(32).

(2) Among the information to be provided by a person filing a commitment in writing pursuant to this Section X.13(b) to allow sale or distribution under Section X.2(a)(1)(B) shall be a commitment that one of the following conditions is true:

(A) the person is a Bona Fide Reseller;

(B) the person is a licensed digital television broadcaster; or

(C) the person is a satellite broadcaster or cable television system operator.

(3) It shall be a violation of this subpart for a person to sell or distribute a Modulation Function pursuant to Section X.13(a)(1)(B) to any person that the person knows, or reasonably should know, does not meet any of the conditions set forth in Section X.13(b)(2).

(4) It shall be a violation of this subpart, enforceable by the Commission, for any person that has filed a written commitment pursuant to this Section X.13(b) to sell or distribute the Modulation Function in the United States other than in accordance with Sections X.13(a)(1)(A) or X.13(a)(1)(B). To the extent that the filing of a written commitment pursuant to this Section X.13(b) creates rights between parties that may be enforced through private contractual remedies or third-party beneficiary rights, enforcement by the Commission will not abrogate those rights and remedies.

(5) The filing of a written commitment will be publicly announced in a timely manner by the Commission, and shall be available in accordance with Secs. 0.441 through 0.470 of this chapter.

#### **X.14 Compliance Requirements for Covered Modulator Products.**

(a) A Covered Modulator Product shall not pass, or direct to be passed, Unknown Content to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output unless it first inspects the EIT and PMT and determines that the Broadcast Flag is not present in such Unknown Content.

(b) A Covered Modulator Product shall not insert the Broadcast Flag into any content.

(c) For the avoidance of doubt, a product shall not be subject to this Section X.14 if and to the extent:

(1) such product is not capable of receiving and modulating Unknown Content; or

(2) the Modulation Function of such product merely:

(A) transcodes a signal from VSB to QAM or from QAM to VSB;

(B) changes the physical channel; or

(C) makes other changes to the signal not affecting the presence or absence of the Broadcast Flag or any other access control or copyright management information;

in each case, regardless of whether or not corresponding changes are made to the PSIP (if present).

### **X.15 Robustness Requirements for Covered Modulator Products: Construction**

(a) Covered Modulator Products shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Covered Modulator Products to defeat the Modulator Compliance Requirements.

(b) Covered Modulator Products shall not include:

- (1) switches, buttons, jumpers or software equivalents thereof,
- (2) specific traces that can be cut, or
- (3) functions (including service menus and remote-control functions),

in each case by which the Modulator Compliance Requirements can be defeated.

**X.16 Robustness Requirements for Covered Modulator Products: Methods of Making Functions Robust.** Covered Modulator Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

(a) **Software.** Without limiting the requirements of Section X.15, portions of a Covered Modulator Product that implement in Software the content protection requirements set forth in the Modulator Compliance Requirements shall be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output of Unknown Content. For purposes of this Section X.16(a), a “modification” includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Section X.15. This Section X.16(a) requires at a minimum the use of signed code or more robust means of “tagging” operating throughout the code. For purposes of this Section X.16(a), “signed code” means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as

effective, to form a digital signature over Software such that its authenticity and integrity can be verified.

**(b) Hardware.** Without limiting the requirements of Section X.15, the portions of a Covered Modulator Product that implement in Hardware the content protection requirements set forth in the Modulator Compliance Requirements shall be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements set forth in the Modulator Compliance Requirements in Covered Modulator Products would pose a serious risk of rendering the Covered Modulator Product unable to receive or modulate Unknown Content. By way of example, a component that is soldered rather than socketed, or affixed with epoxy, may be appropriate for this means.

**(c) Hybrid.** The interfaces between Hardware and Software portions of a Covered Modulator Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection that would be provided by a pure Software implementation.

**X.17 Robustness Requirements for Covered Modulator Products: Level of Protection.** The content protection requirements set forth in the Modulator Compliance Requirements shall be implemented in a reasonable method so that they:

**(a)** Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons, or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers, other than Circumvention Devices; and

**(b)** Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section X.17(a) such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

**X.18 Robustness Requirements for Covered Modulator Products: Advance of Technology.** Although an implementation of a Covered Modulator Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Covered Modulator Product, would have caused such products to fail to comply with these Modulator Robustness Requirements (“New Circumstances”). If a manufacturer of a Covered Modulator Product has actual notice or actual knowledge of New Circumstances that

relate to the manufacturer's specific implementation of a Covered Modulator Product (hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such manufacturer shall cease distribution of such Covered Modulator Product and shall only distribute Covered Modulator Products that are compliant with the Modulator Robustness Requirements in view of the then-current circumstances.

**X.19 Authorization for Use With Unscreened Content.** In order to be authorized for use with Unscreened Content, an Authorized Digital Output Protection Technology or Authorized Recording Method must, in addition to meeting other applicable criteria, further either:

(1) protect Unscreened Content in a manner that prohibits its digital recording (other than temporary storage solely for the purpose of enabling immediate or delayed display) unless and until the EIT or PMT for content contained in a stream that has not been altered following demodulation is inspected for the Broadcast Flag, in which case:

(A) if the Broadcast Flag is determined to be present, the content shall thenceforth be treated in the same manner as if it had been passed from a Covered Demodulator Product protected by such Authorized Digital Output Protection Technology (pursuant to X.4(a)(3) or X.6(b)), or recorded using such Authorized Recording Method (pursuant to X.4(b)(2)), as Marked Content; and

(B) if the Broadcast Flag is determined not to be present, no protections are thenceforth required to apply; or

(2) protect Unscreened Content so that such content may be accessed in usable form by another product only if such other product protects such content in accordance with the Compliance and Robustness Requirements applicable to Unscreened Content, as if it were a Covered Demodulator Product.

# **ATTACHMENT C**

December 6, 2002

**Joint Proposal from MPAA and 5C Companies  
for Table A Criteria**

This proposal is being made to the Commission to suggest criteria for adoption by the Commission to authorize digital output and recording technologies for Table A.

**Notes:**

- Authorization of a given technology will generally require the inclusion of “Associated Obligations” (as defined below) in Table A, which will pertain to the use of that technology by a Covered Product to protect Unscreened Content or Marked Content against unauthorized redistribution (including unauthorized Internet redistribution).
- This proposal contemplates that the criteria set forth below will be used in connection with processes to be determined by the Commission for adding technologies to Table A after adoption of the regulation promulgating the compliance and robustness requirements. Notwithstanding, the proponents recommend that the Commission authorize technologies for protecting digital output and recording of protected DTV content, in such manner that the Compliance and Robustness Requirements do not take effect prior to the authorization of technologies that enable such content to be passed and recorded in accordance with the Requirements.
- This proposal recommends that the Commission address the following issues:
  - i) A process by which (a) a party can file a notice demonstrating that any of the criteria is met, which notice would, where applicable, specify which companies have used or approved a technology as contemplated in the criteria; (b) each company named in the notice as having used or approved a technology is given adequate opportunity to dispute the facts alleged in the notice with respect to such company’s use or approval, and (c) any such disputes can be swiftly resolved.
  - ii) A process by which (a) a party can file a notice seeking information as to whether one or more companies have “used” or “approved” a technology, as “use” and “approval” are defined below; and (b) each company named in the notice is required to respond as to whether or not it has “used” or “approved” the technology.
  - iii) A process for ensuring that a listed technology that has been significantly compromised in relation to its ability to protect Unscreened Content and Marked Content from unauthorized redistribution (including unauthorized Internet redistribution) will not be used as a technology for “at least as effective” evaluation pursuant to criterion (3), below.

- iv) A standard by which a technology could be removed from the list where such technology has been compromised (where the level of “compromise” is substantially higher than the level required for the process contemplated in paragraph iii, above), which standard would take into account the protection of Unscreened Content and Marked Content from unauthorized redistribution (including from unauthorized Internet redistribution), and the impact on content owners, consumers and manufacturers resulting from the continued use of such compromised technology and from any removal of such technology from the list. This proposal recommends that the Commission will address a process by which (a) requests can be made to remove a technology from the list on the basis that such standard has been met; (b) interested parties can object to such requests for removal; and (c) a timely determination would be made as to whether or not such technology will be removed from Table A (after a reasonable grace period).
- v) The appropriate entity or entities that would administer Table A and the processes described above.

- This proposal also recommends that the Commission address the issue of the applicable grace period before the Compliance and Robustness Requirements become effective.
- Definitions for capitalized terms not otherwise defined herein will need to be defined.

**Proposed Criteria:**

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) The technology is at least as effective at protecting Unscreened Content and Marked Content against unauthorized redistribution (including unauthorized Internet redistribution) as is any one of the technologies then listed on Table A (other than technologies then deemed to be “significantly compromised” pursuant to the process contemplated in clause (iii) in the note above). A determination of whether a technology is “at least as effective” requires 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.<sup>1</sup> For purposes of this criterion, at the initiation of the licensor of the technology or of another company, a public notice will be issued providing 60 days for comment on the request to include such technology on Table A. In the event that the licensor of such technology is not the initiator of the request and objects within such 60-day period to the inclusion of such technology on Table A, then such technology shall not be included on Table A. In the event that the licensor of such technology does not object within such 60-day period but 3 Major Studios and/or Major Television Broadcast Groups object, during the 60-day public notice period, to the inclusion of such technology on Table A on the basis that such technology does not meet this criterion, the matter shall be resolved through an expedited process (not to exceed an additional 45 days) to determine whether or not the criterion is satisfied. In connection with such determination, evidence that the technology is in legitimate use in a Major Commercial Market in connection with the output or recording of a commercially significant amount of New Release Content shall weigh in favor of a determination that such technology is “at least as effective” as a technology then on Table A, provided that if such technology has not been so used in connection with a commercially significant amount of New Release Content, such fact shall not be weighed against a finding that such technology meets such “at least as effective” standard.<sup>2</sup> In the event that there are fewer than 3 Major Studios and/or Major Television Broadcast Groups that so object within the specified period of time (and the licensor of the technology does not object) or if the result of the expedited process is a determination that the technology meets this criterion, then the technology will be included on Table A. If the result of the expedited process is a determination that the technology does not meet this criterion or the licensor of the technology objects, at any time prior to the conclusion of such process, to the inclusion of its technology on Table A, then the technology will not be included on Table A. For purposes of satisfying this criterion, if any Major Studio or Major Television Broadcast Group is counted as objecting to the inclusion of such technology on Table A, no Affiliate of such counted entity may also be counted as so objecting.

- (4) The technology (together with its license terms) includes output and recording controls that protect against unauthorized redistribution of audiovisual content (including unauthorized Internet redistribution) and such technology was expressly named as being permitted to be used for the output or recording (as applicable) of audiovisual content (except where such permission does not extend

---

<sup>1</sup> The proponents understand that other parties may support the establishment of additional or variations of the objective criteria for this criterion 3. The proponents look forward to discussing such proposals with such other parties in greater detail.

<sup>2</sup> By way of example and not limitation, a technology shall not be deemed to be in use “in connection with the output or recording of a commercially significant amount of New Release Content” if: (i) such use is solely for internal testing or other evaluation of such technology (including but not limited to testing or evaluation in the form of limited-duration “beta testing”); (ii) the company or companies that use such technology demonstrate their intent to use such technology solely outside the United States; or (iii) such use relates solely to the non-commercial distribution of audiovisual content, such as distribution solely to professional devices or for internal distribution within a company (including its Affiliates).

to use in connection with New Release Content) under the license applicable to a technology listed on Table A (whether such license itself expressly names the technology or references another means by which such technology may be expressly named), either (a) at the time such listed technology was listed on Table A, or (b) at a later date, provided that a Change Management process applied to such subsequent naming of such technology and such subsequent naming complied with such Change Management process.

A failure to satisfy any of the above criteria shall not preclude the subsequent addition of the technology to Table A pursuant to that or any other criteria.

For purposes of criteria (1) and (2) (and for no other purpose, e.g., not for purposes of patent law), a company shall be deemed to have “used” or “approved” a technology (a “Proposed Table A Technology”) only if such technology (together with its license terms) includes output and recording controls that protect against unauthorized redistribution of audiovisual content (including unauthorized Internet redistribution) and:

(a) such company or, where such company is a Major Studio, any of its Qualified Affiliates, has signed an agreement with the licensor of such Proposed Table A Technology that expressly authorizes (including, for avoidance of doubt, via license grant, non-assertion covenant or other authorization) the company or any of the company’s Qualified Affiliates (either immediately or upon a specified future date or circumstance) to use or cause the use of such Proposed Table A Technology in a Major Commercial Market, in connection with the output or recording (as applicable) of audiovisual content (except where such authorization does not extend to use in connection with the company’s New Release Content), provided that the use of such Proposed Table A Technology was expressly provided for in such agreement at the time the company enters into such agreement (whether such agreement then permits the use of the Proposed Table A Technology or then specifies a future date or circumstance upon which such use of such Proposed Table A Technology shall be permitted), and provided further that such “use” or “approval” shall not be deemed to exist prior to the effective date of any right to use such Proposed Table A Technology under such agreement;

(b) such company or, where such company is a Major Studio, any of its Qualified Affiliates, has entered into a content license or similar content-related agreement that, upon signature (and not pursuant to a Change Management procedure), expressly identifies, either directly, or indirectly by description or reference, such Proposed Table A Technology (i.e., by expressly naming such technology in such content license or content-related agreement or, indirectly, by expressly naming such technology in a specification, standard or license that is directly or indirectly linked by explicit reference through one or more instruments to such content license or content-related agreement) as being permitted to be used for the output or recording (as applicable) of the company’s audiovisual content (except where permission does not extend to use in connection with the company’s New Release Content);

(c) such company or, where such company is a Major Studio, any of its Qualified Affiliates, has signed an agreement with the licensor of another technology for which the applicable license specifically permits the use (either immediately or upon a specified future date or circumstance) of the Proposed Table A Technology in a Major Commercial Market in connection with the output or recording of audiovisual content (except where such permission does not extend to use in connection with the company's New Release Content), provided that the use of such Proposed Table A Technology was expressly provided for in such agreement at the time the company enters into such agreement (whether such agreement then permits the use of the Proposed Table A Technology or then specifies a future date or circumstance upon which such use of such Proposed Table A Technology shall be permitted) and provided further that such "use" or "approval" shall not be deemed to exist prior to the effective date of any right to use such Proposed Table A Technology under such agreement;

(d) such company has issued an unambiguous public statement endorsing the Proposed Table A Technology for the output or recording (as applicable) of the company's audiovisual content (except where such endorsement does not extend to use in connection with the company's New Release Content) or the inclusion of the Proposed Table A Technology on Table A; or

(e) a General Counsel or equivalent legal representative of such company has approved in writing the inclusion of the Proposed Table A Technology on Table A.

By way of example and not limitation, a company shall not be deemed to have "used" or "approved" a technology if: (i) its use or approval relates solely to internal testing or other evaluation of such technology (including but not limited to testing or evaluation in the form of limited-duration "beta testing"); (ii) notwithstanding any contractual right to use such technology for New Release Content, the company demonstrates that it uses and intends to use such technology under such contract solely in connection with content other than New Release Content; (iii) the company demonstrates its intention to use or approve the use of the technology solely outside the United States; or (iv) its use or approval relates solely to the non-commercial distribution of audiovisual content, such as distribution solely to professional devices or for internal distribution within the company (including its Affiliates).

An entity that is counted to satisfy a criterion cannot be counted more than once in satisfying that criterion.

For purposes of satisfying criterion 1 or 2, if an entity is counted as a Major Device Manufacturer, Major Studio, or Major Television Broadcast Group (each, an "Industry Category"), no Affiliate of such counted entity may be counted in the same or any other Industry Category, except that (a) if an entity is counted as a Major Device Manufacturer, 1 Affiliate of such counted entity may be counted as either a Major Studio or Major Television Broadcast Group; and (b) if an entity is counted as a Major Studio or

Major Television Broadcast Group, 1 Affiliate of such counted entity may be counted as a Major Device Manufacturer.

“Affiliate” means, with respect to any entity, any corporation, partnership or other entity that, directly or indirectly, owns, is owned by, or is under common ownership with, such first entity, for so long as such ownership exists. For purposes of the foregoing, “own,” “owned” or “ownership” shall mean holding ownership of, or the right to vote, more than fifty percent (50%) of the voting stock or ownership interest entitled to elect a board of directors or a comparable managing authority.

“Change Management,” for purposes of these criteria, means a process by which content owners are provided a specified right or ability to meaningfully object to particular amendments to content protection agreements.

“Major Commercial Markets,” for purposes of these criteria, means the United States, any country within the European Community, Canada, Japan and Australia.

“Major Device Manufacturer,” for purposes of these criteria, means any member of CEA, ITI, BSA or CCIA, the total gross revenues of which from device manufacturing and software publishing exceed US\$ \_\_\_\_\_ per year.

“Major Studio,” for purposes of these criteria, means, during the course of any year, any member of the MPAA or any other company that has generated U.S. box office revenues from theatrical releases of feature films in the immediately prior year that are at least as great as the MPAA member company with the lowest U.S. box office revenues from theatrical releases of feature films for that same year.

"Major Television Broadcast Group," for purposes of these criteria, means the 4 largest broadcast networks and the 5 largest television station groups that are not affiliated with Major Studios.

“New Release Content,” for purposes of these criteria, means, with respect to the application of any Proposed Table A Technology to audiovisual content, audiovisual content owned or acquired by license (with the right to determine distribution methods) by a Major Studio and first commercially released during the 24-month period preceding such application of such technology to such audiovisual content.

“Qualified Affiliate” means, with respect to a Major Studio, (a) an entity that directly or indirectly owns and controls such Major Studio or (b) an Affiliate of a Major Studio authorized to distribute the preponderance of the New Release Content owned or licensed by such Major Studio for one or more of the major content distribution channels (i.e., theatrical, home entertainment, pay-per-view, video-on-demand, pay television, basic cable or broadcast television). For purposes of the foregoing, “own” shall mean holding ownership of, or the right to vote, more than fifty percent (50%) of the voting stock or ownership interest entitled to elect a board of directors or a comparable managing authority.

# **ATTACHMENT D**

Table A

[Anticipates list setting forth specific technologies together with any Associated Obligations.]

| Authorized Digital Output Protection Technologies | Associated Obligations | Authorized for Use with Unscreened Content: Yes/No |
|---|------------------------|--|
|   |                        |  |
|   |                        |  |
|   |                        |  |

| Authorized Recording Methods | Associated Obligations | Authorized for Use in Connection with Removable Media: Yes/No | Authorized for Use with Unscreened Content: Yes/No |
|------------------------------|------------------------|---|--|
|                              |                        |   |  |
|                              |                        |   |  |
|                              |                        |   |  |