

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

<b>In the Matter of</b>	)	
	)	
<b>Digital Broadcast Content Protection</b>	)	<b>MB Docket No. 02-230</b>
	)	

**OMNIBUS REPLY OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.  
TO THE OPPOSITIONS FILED BY ATI TECHNOLOGIES, INC.,  
THE CONSUMER ELECTRONICS INDUSTRY, THE IT COALITION, THE  
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION, AND  
PUBLIC KNOWLEDGE & CONSUMERS UNION**

Jon A. Baumgarten  
Bruce E. Boyden  
Proskauer Rose LLP  
1233 Twentieth Street NW, Suite 800  
Washington, DC 20036  
(202) 416-6800

March 22, 2004

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

**TABLE OF CONTENTS**

	<u>Page</u>
INTRODUCTION AND SUMMARY .....	1
I. The Commission Should Adopt the Jointly Proposed Robustness Rules.....	3
A. The Robustness Rules Must Deter Attacks by Experienced Hackers.....	4
B. High-Value Content Broadcast Digitally Over-the-Air Must Be Protected to Achieve the Commission’s Goal .....	8
C. The Jointly Proposed Robustness Rules Would Not Burden Manufacturers.....	10
D. The Jointly Proposed Robustness Rules Will Not Burden MVPDs .....	12
E. The Jointly Proposed Robustness Rules Are Standard in the Market for the Protection of High-Value Content .....	13
II. Section 73.9006 of the Commission’s Rules Must Be Corrected.....	14
CONCLUSION.....	16

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

<b>In the Matter of</b>	)	
	)	
<b>Digital Broadcast Content Protection</b>	)	<b>MB Docket No. 02-230</b>
	)	

**OMNIBUS REPLY OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.  
TO THE OPPOSITIONS FILED BY ATI TECHNOLOGIES, INC.,  
THE CONSUMER ELECTRONICS INDUSTRY, THE IT COALITION, THE  
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION, AND  
PUBLIC KNOWLEDGE & CONSUMERS UNION**

**INTRODUCTION AND SUMMARY**

The Motion Picture Association of America, Inc. (“MPAA”) submits this omnibus reply to the Oppositions filed by ATI Technologies, Inc., the Consumer Electronics Industry, the IT Coalition, the National Cable & Telecommunications Association, and Public Knowledge & Consumers Union to its Petition for Reconsideration<sup>1</sup> of certain aspects of the Commission’s Broadcast Flag regulation.<sup>2</sup> In particular, the MPAA requested that the Commission reconsider its decision not to adopt the set of robustness rules – the “Jointly Proposed Robustness Rules” – drafted by the MPAA, the 5C companies,<sup>3</sup> and the Computer Industry Group (“CIG”), and discussed in the Broadcast Protection Discussion Group (“BPDG”).<sup>4</sup> Essentially the same

---

<sup>1</sup> See Petition for Reconsideration and Clarification of the Motion Picture Association of America, Inc. (“MPAA Petition”) (filed Jan. 2, 2004).

<sup>2</sup> See Report and Order and Further Notice of Proposed Rulemaking, *Digital Broadcast Content Protection*, M.B. Docket No. 02-230, FCC 03-273 (rel. Nov. 4, 2003) (“Broadcast Flag Order”).

<sup>3</sup> The “5C companies” are the five member companies of the Digital Transmission Licensing Authority (“DTLA”), namely, Intel Corp., Hitachi Ltd., Matsushita Electric Industrial Co. Ltd., Sony Electronics Inc., and Toshiba Corp.

<sup>4</sup> See Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group (“BPDG Report”), June 3, 2002, Tab F-2 §§ X.7 – X.11 & “Note to Reader.”

robustness rules were proposed by 5C and MPAA in this proceeding, and are attached to the MPAA Petition at Exhibit A. Second, the MPAA requested that the Commission correct Section 73.9006 in order to clarify that Marked and Unscreened Content are not to be made available in unencrypted, compressed form via a User Accessible Bus.

In response, several parties have objected to the Jointly Proposed Robustness Rules. For example, several parties claimed that the Jointly Proposed Robustness Rules are not necessary to create the “speed bump” to unauthorized redistribution that the Commission intended. However, as explained below, the past experience of licensees and licensors of content protection technologies demonstrates conclusively that robustness rules such as the Jointly Proposed Robustness Rules are precisely what is required. Others objected that free over-the-air digital television was not worthy of the same level of robustness used to protect content in other distribution channels. However, such comments overlook the entire point of this proceeding, which is to “ensure the continued availability of high value DTV content to consumers through broadcast outlets.”<sup>5</sup> As the MPAA and others have demonstrated previously, high-value content will migrate to other distribution channels unless over-the-air digital broadcast television receives an equivalent level of protection.

Some parties objected that the Jointly Proposed Robustness Rules would impose too high a burden on manufacturers. These comments ignore the fact that the Jointly Proposed Robustness Rules are already commonplace requirement for products that securely handle high-value content, and components implementing such robustness rules are in place in a multitude of consumer products today. That is why the Jointly Proposed Robustness Rules received

---

<sup>5</sup> Broadcast Flag Order ¶ 8.

“[g]eneral agreement” in the BPDG.<sup>6</sup> Furthermore, the Jointly Proposed Robustness Rules will impose no great burdens on cable operators, either. In fact, they are very similar to those already contained in the DFAST and PHILA licenses, to which cable operators have already agreed.

Finally, the Commission should restore the original intent of the second sentence of Section 73.9006 as developed in the BPDG and clarify that Marked and Unscreened Content must not be made available in unencrypted, compressed form via a User Accessible Bus.

### **I. The Commission Should Adopt the Jointly Proposed Robustness Rules**

In its Petition for Reconsideration, the MPAA provided detailed reasons why the Commission should adopt the Jointly Proposed Robustness Rules. First, the Jointly Proposed Robustness Rules are necessary in order to ensure that the Commission’s goal of protecting the viability of over-the-air broadcast television is achieved. As has been demonstrated with respect to other content distribution channels such as DVDs as well as other industries, implementing a “speed bump”<sup>7</sup> for the unauthorized redistribution of content requires thwarting not just attacks by ordinary users, but attacks by persons using professional tools as well. Second, the Jointly Proposed Robustness Rules are very similar to those already implemented in numerous products under existing content protection agreements, thus ensuring that digital broadcast television will receive an equivalent level of protection. Finally, the Jointly Proposed Robustness Rules will result in no undue burdens on manufacturers, as evidenced by the fact that they are already complying with such rules in other arenas. None of the oppositions to the MPAA Petition have refuted any of these points.

---

<sup>6</sup> BPDG Report ¶ 4.9.

<sup>7</sup> Broadcast Flag Order ¶ 14.

**A. The Robustness Rules Must Deter Attacks by Experienced Hackers**

Some of the oppositions to the MPAA Petition cited the Commission’s goal in providing a “speed bump” for the unauthorized redistribution of content as a reason why the Commission should reject the Jointly Proposed Robustness Rules.<sup>8</sup> The notion of a “speed bump,” rather than a “vault” or a “safe,” implies that the product will hamper attempts to gain access to digital content in the clear, but is not required to absolutely prevent it. Thus, contrary to what the oppositions assume, the notion of a “speed bump” does not *per se* imply the use of the “ordinary user” standard as opposed to a higher level of robustness. As the MPAA demonstrated in its Petition, there are two types of attacks a product must deter to provide even an effective “speed bump” for unauthorized redistribution.<sup>9</sup> First, the product must implement the Broadcast Flag compliance rules – Sections 73.9003 through 73.9006 – in a “reasonable method” that ensures that they “[c]annot be defeated or circumvented” by using either general-purpose or specialized tools “widely available at a reasonable price.”<sup>10</sup> Second, the product must implement the compliance rules in a reasonable method that ensures that those rules can be defeated or circumvented “only with difficulty . . . using professional tools or equipment . . . such as would be used primarily by persons of professional skill and training.”<sup>11</sup> That is, attacks with professional tools and equipment must be reasonably difficult. Even the CE Industry supports prevention of these two sorts of attacks, which are, as CE notes, “a familiar requirement for consumer electronics and information technology products.”<sup>12</sup> The same could be said for all of

---

<sup>8</sup> See Objections to the “Petition for Reconsideration and Clarification of the MPAA” of ATI Technologies, Inc. (“ATI”) at 4; Opposition to Petitions for Reconsideration of the IT Coalition (“IT”) at 3; The National Cable & Telecommunications Association’s Opposition to Petitions for Reconsideration (“NCTA”) at 4.

<sup>9</sup> See MPAA Petition at 11-15.

<sup>10</sup> MPAA Petition at 10.

<sup>11</sup> MPAA Petition at 10-11.

the Jointly Proposed Robustness Rules contained in Sections X.7 to X.12; they are all “familiar requirements” for both IT and CE products, as the MPAA has demonstrated.<sup>13</sup>

CE states further that the FCC should acknowledge that “Robustness does not require absolute security from attack.”<sup>14</sup> The same is true of the Jointly Proposed Robustness Rules. For example, Section X.11 requires only that products be implemented in a “reasonable method” such that they can “only with difficulty” be defeated or circumvented with professional tools, and provides further that Covered Products are not required to be secure against Circumvention Devices as defined in the proposal. Section X.7(a) requires only that products be designed to effectively “frustrate” attempts to compromise their security, not that they in practice actually “prevent” all attempts to compromise their security. Obviously, absolute prevention of compromises is not required.<sup>15</sup> Under the Jointly Proposed Robustness Rules, there may still be compromises, but there will be far fewer of them, just as is the case with other, protected distribution channels.

None of the oppositions successfully defended the “ordinary user” standard. First of all, Public Knowledge is simply incorrect when it argues that ordinary users could not implement attacks distributed by others because “[t]he ordinary user does not download complex . . . software, navigate often difficult to understand software and menus, store massive files on his or

---

<sup>12</sup> Consumer Electronics Industry Opposition to Petitions for Reconsideration (“CE”) at 2; *see also* Comments of Philips Electronics North America Corporation on Further Notice of Proposed Rulemaking at 14-15 (filed Feb. 13, 2004).

<sup>13</sup> *See* MPAA Petition at 9-17.

<sup>14</sup> CE at 3.

<sup>15</sup> Public Knowledge and Consumers Union miss this point. *See* Opposition to Petitions for Reconsideration of Public Knowledge and Consumers Union (“PK/CU”) at 8 (opposing “raising an impenetrable robustness wall based on the broadcast-flag scheme”).

her hard drive and then post these massive files for redistribution.”<sup>16</sup> Quite to the contrary, millions of “ordinary users” have downloaded illegal file trafficking programs for the purpose of engaging in unauthorized redistribution of copyrighted works. It is clear that the proliferation of compromises of DTV products is a real threat with which the Commission must be concerned. Second, Public Knowledge’s reading of the Commission’s “robustness” standard effectively empties the concept of any meaning. Under Public Knowledge’s understanding, a case screw is robust, since as Public Knowledge notes, “the ordinary user is not prone to open his or her expensive consumer electronics equipment.”<sup>17</sup> Such a standard is plainly inadequate, as the Commission has previously recognized.<sup>18</sup>

Nevertheless, even if Public Knowledge’s interpretation is rejected, it is still far from clear that both of the two types of attacks mentioned above (i.e., downloading of published hacks and the dismantling of a computer) would be protected against under the “ordinary user” standard. For example, the National Cable & Telecommunications Association (“NCTA”) states that it does not accept that the “ordinary user” standard would fail to apply to the use of hacks to circumvent the compliance rules of devices.<sup>19</sup> The problem, however, is that while designers under such a robustness rule would obviously have to build their devices to be secure against *past* compromises available to ordinary users, it is less certain that they would have to build their devices to be secure against *future* compromises by experts who would then distribute the hack. The Jointly Proposed Robustness Rules solve this problem by providing two standards, one for

---

<sup>16</sup> PK/CU at 7.

<sup>17</sup> *Id.* Public Knowledge also repeatedly chides the MPAA for not introducing new evidence to support its petition for reconsideration. *See* PK/CU at 2, 8, 9. Not only is new evidence not required for a petition for reconsideration, it is presumptively disfavored, and allowed by the Commission only in certain circumstances. *See* 47 C.F.R. § 1.429(b).

<sup>18</sup> *See* 47 CFR § 15.121(a)(1).

the use of widely available tools and one for professional tools, and further provide a set of specific guidelines for device manufacturers to follow in meeting these standards.

As the MPAA argued in its Petition, the creation and widespread distribution of the DeCSS hack of the CSS encryption system that protects DVDs is proof that products must be robust against not only attacks by ordinary users, but by experts as well. Several oppositions, however, argued that the existence of DeCSS proved just the opposite: that a *lower* standard of robustness is permissible, since DVDs are still profitable. For example, IT suggested that the DeCSS example proves that “the FCC’s intended ‘speed bump’ system of content protection is more than adequate to address indiscriminant redistribution of video content.”<sup>20</sup> This response misses the point of the example. The CSS license contains robustness rules very similar to those of the Jointly Proposed Robustness Rules. *Even so, there has unfortunately been a single successful compromise by skilled attackers that was virally spread in the form of an executable download.* Fortunately, because of the CSS robustness rules, that one situation has not recurred and has been successfully countered through legal action,<sup>21</sup> which is why “its availability has not led to its widespread use by the ordinary user.”<sup>22</sup> Imagine, however, if the CSS license had contained a lower standard of robustness; such a standard would likely lead to multiple compromises that as a practical matter may test the ability of litigation to successfully combat them. Far from providing a “speed bump” to redistribution, it would in fact provide a steep

---

<sup>19</sup> NCTA at 3-4.

<sup>20</sup> IT at 7; *see also* PK/CU at 7. The IT Coalition also suggests, citing a single article, that most unauthorized redistribution of high-value content will come not from compromised devices but from “inside” sources. *See* IT at 8 n.15. The study cited by the IT Coalition is based on deeply flawed premises and methodology, however, and its conclusions should not be accepted as fact.

<sup>21</sup> *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *Paramount Pictures Corp. v. 321 Studios*, 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 2004 WL 415250 (N.D. Cal. Feb 19, 2004).

<sup>22</sup> PK/CU at 7.

downward slope. That is the result the Commission must avoid.

**B. High-Value Content Broadcast Digitally Over-the-Air Must Be Protected to Achieve the Commission's Goal**

Two oppositions claimed that a lower robustness standard is required for broadcast television devices because the broadcast television signal is not encrypted at the source.<sup>23</sup> The robustness standard to be required of DTV products has nothing to do with whether broadcast television content is encrypted at the source. No matter how it is delivered to the DTV receiver, that receiver must be secure against the defeat or circumvention of its compliance rules in order for the Broadcast Flag system to be effective. As a delivery mechanism for high-quality content, there is no reason to believe that digital television receivers will not be the targets of attacks. Furthermore, the Commission is well aware of the reasons why digital broadcast television could not be encrypted at the source. Among other problems, “the obsolescence of legacy equipment” would have been “particularly burdensome on consumers,” and the delay in implementing an encryption scheme would have delayed the digital transition.<sup>24</sup> The Commission should not allow its accommodation of legacy devices and the necessity of a prompt digital transition to be used as an argument that the Commission’s policy goal – protection of broadcast television content equivalent to that received in other distribution channels – should not be attempted.

Similarly, the threat of the construction of non-compliant demodulators does not support a lower standard of robustness for those products that are compliant.<sup>25</sup> Such claims overlook the critical fact that noncompliant demodulators will be *illegal* under the regulation. The fact that some people may break the law and distribute *noncompliant* demodulators does not mean that

---

<sup>23</sup> See IT at 4-5; NCTA at 2.

<sup>24</sup> Broadcast Flag Order ¶ 24.

<sup>25</sup> See ATI at 3-4; IT at 5 n.9; NCTA at 3.

*compliant* demodulators should not have to meet the same robustness standards as devices that handle content delivered in competing distribution channels. If the Commission accepts the argument of the oppositions on this issue, it risks the very migration of content to other, protected channels that it set out in this proceeding to forestall.

The fact that the Broadcast Flag regulation allows copying of Marked and Unscreened Content is also irrelevant to the question of the proper level of robustness.<sup>26</sup> The purpose of robustness is not to prevent copying, but to ensure that, whatever the applicable compliance rules are for each type of content, they are followed. The compliance rules for over-the-air digital broadcast television allow copying, while those for some other distribution channels do not, but this fact is irrelevant. If anything, given the places to which the content can flow, robustness in ensuring that all of those compliance rules are met is *more important* for digital broadcast television receivers, not less important.

Many of the above objections to the Jointly Proposed Robustness Rules are premised, explicitly or implicitly, on the notion that digital broadcast television is not entitled to the same level of protection as other distribution channels.<sup>27</sup> Such comments are made without regard to the Commission's findings and miss the entire point of the Broadcast Flag regulation, which is to afford digital broadcast television content a level of protection *equivalent* to that received by content on other distribution channels, so that high-value content will not migrate to those other venues. Allowing over-the-air television to become less secure than other forms of distribution will thus threaten the viability of over-the-air broadcast television.

---

<sup>26</sup> See IT at 3-4; NCTA at 3.

<sup>27</sup> See IT at 3-4; NCTA at 3 (objecting that the Jointly Proposed Robustness Rules would make DTV receivers as secure as DFAST devices).

### C. The Jointly Proposed Robustness Rules Would Not Burden Manufacturers

The IT Coalition claims that compliance with the Jointly Proposed Robustness Rules would be overly burdensome and would “needlessly increase costs for both device manufacturers and consumers and likely stifle innovation.”<sup>28</sup> However, there are millions of products available for sale to consumers in the marketplace at this very moment that comply with robustness rules equivalent to those contained in the Jointly Proposed Robustness Rules. All DVD players and drives, for example, comply with the robustness rules contained in the CSS Specifications, which are nearly identical to those contained in the Jointly Proposed Robustness Rules. Given that CE and IT manufacturers have had no difficulty in developing innovative products that meet such robustness rules and offering them to consumers for reasonable prices, it cannot seriously be suggested that it will be impossible or even burdensome for manufacturers to comply with the Jointly Proposed Robustness Rules.<sup>29</sup>

Furthermore, the IT industry’s complaints at this stage are particularly perplexing, given that changes to the Jointly Proposed Robustness Rules were made *specifically to accommodate IT’s concerns*. Section X.6, allowing Robust Methods<sup>30</sup> for transfers from add-in computer

---

<sup>28</sup> ATI Technologies claims that the Jointly Proposed Robustness Rules would require a demodulator to determine if a downstream device can be trusted, which can only be done through cryptography. *See* ATI at 2. However, it is the Compliance Rules, not the Robustness Rules, that determine how content is passed from a product; and while the Demodulator Product as a whole must ensure that content passed over a digital connection is securely passed, in most cases that task will be performed by the Authorized Digital Output Protection Technology.

<sup>29</sup> While the members of the IT Coalition might have experience in the cost of building devices, it is also an interested party, and the objective evidence of the cost of implementing robustness rules similar to the Jointly Proposed Robustness Rules refutes its claims of unacceptable burdens. *See* IT at 5.

<sup>30</sup> The definition of “Robust Method” in the Jointly Proposed Robustness Rules differs from that adopted by the Commission. *See* MPAA Petition at 8-9. In the Jointly Proposed Robustness Rules, a Robust Method is not simply a method that complies with the other robustness rules, but is defined in Section X.10:

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,

products, was added during the BPDG discussions precisely to address IT’s concern that compliance with the compliance rules would represent in some cases too heavy a burden for open-architecture computer products. Having accepted that compromise, IT is now claiming that even compliance with Robust Methods, as then understood, is an impossible burden, and that it cannot possibly build anything more secure than the “ordinary user” standard. IT’s claims in this regard are not credible.<sup>31</sup>

Finally, whatever the IT Coalition’s opinion of the Jointly Proposed Robustness Rules is now, IT’s issues with those rules were evidently so obscure that not only did the IT industry not oppose them during the BPDG process, but it actively supported the Jointly Proposed Robustness Rules. That support was not conditioned, as the IT Coalition now suggests, on amendment of the robustness rules to include an “ordinary user” standard,<sup>32</sup> and it was not limited to the April 25, 2002 “Discussion Draft,”<sup>33</sup> but extended all the way through to the BPDG Final Report. IT’s opposition to the Jointly Proposed Robustness Rules now does not give it the ability to retroactively alter the record in this respect. In the Final Report of the BPDG, the IT industry demurred on only two points in the entire Joint Proposal: first, that “additional or variations of the objective criteria” contained in the “at least as effective” criterion be considered; and second, that “the Compliance and Robustness Requirements not go into effect until a minimum number

---

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 [Peripheral TSP] Product.

<sup>31</sup> See MPAA Petition at 7 & n.15.

<sup>32</sup> See IT at 6.

<sup>33</sup> See IT at 4 n.7.

of technologies have been included in Table A.”<sup>34</sup> The “ordinary user” standard has evidently not always been as critical to the IT industry as the IT Coalition now is claiming.

ATI Technologies has objected that the Jointly Proposed Robustness Rules would impose a burden on manufacturers by requiring demodulators and decoders to be sold together.<sup>35</sup> In fact, however, this is not the case. Section 73.9003(a)(4) of the Broadcast Flag regulation permits the sale of Peripheral TSP Products<sup>36</sup> in which the demodulation and processing functions are separated. Furthermore, even within a single product, the demodulation and processing functions do not all need to be housed on the same components.<sup>37</sup> The Broadcast Flag regulation, including the Jointly Proposed Robustness Rules, permits manufacturer innovation in designing their products.

**D. The Jointly Proposed Robustness Rules Will Not Burden MVPDs**

NCTA raises the specter that the Jointly Proposed Robustness Rules would somehow convert the Broadcast Flag into “a tool by which MPAA, its member studios, or anyone else passing judgment on robustness or robust connections could control every element of an MVPD’s transport and the architecture of a secure home network.”<sup>38</sup> Since the robustness rules will be interpreted primarily by the Commission, and enforceable only through the Commission’s or a court’s order, NCTA’s professed fear is inherently unreasonable. In any

---

<sup>34</sup> See BPDG Final Report ¶¶ 6.8, 6.9.

<sup>35</sup> See ATI at 3.

<sup>36</sup> Under Section 73.9000(j), a “Peripheral TSP Product” means “a product that is capable of accessing in usable form Unscreened Content or Marked Content passed to such product via a Robust Method where the manufacturer of such product has committed in writing in accordance with § 73.9002(c) that such product will comply with the Demodulator Compliance Requirements and be manufactured in accordance with the Demodulator Robustness Requirements.”

<sup>37</sup> See Joint Reply Comments of the MPAA *et al.* at 24 (filed Feb. 20, 2003); Reply Comments of Thomson Inc. at 2-3 (filed Feb. 18, 2003).

event, the level of robustness contained in the Jointly Proposed Robustness Rules is very similar to that cable operators have already agreed to in the DFAST and PHILA licenses, without ill effects.

**E. The Jointly Proposed Robustness Rules Are Standard in the Market for the Protection of High-Value Content**

The MPAA cited numerous multi-lateral agreements between CE, IT, cable, and content owners that contain almost exactly the same robustness rules as are contained in the Jointly Proposed Robustness Rules. Those robustness rules have ultimately been embraced by consumers, who have purchased products manufactured in accordance with them in large numbers. The IT Coalition’s only response to this wealth of evidence is that such agreements are “simply private license agreements” and therefore are not “market agreements.”<sup>39</sup> It is unclear, however, what the IT Coalition’s conception of a “market agreement” is, if it does not include the vast majority of the agreements negotiated between private parties in the market for the distribution of high-value content. Similarly, Public Knowledge dismisses such agreements as “studio-dominated agreements that primarily reflect the content industries’ desires,”<sup>40</sup> but that will surely come as news to the CE, IT, cable, and satellite companies that were parties to them, or the consumers who have purchased such products in droves. Despite what Public Knowledge and the IT Coalition claim, it is clear that in the free market, content protection technology licenses for the protection of high-value content include robustness rules much like the Jointly Proposed Robustness Rules. Indeed, the MPAA in its Petition for Reconsideration cited multiple precedents for each of the rules. The Commission should recognize this marketplace standard

---

<sup>38</sup> NCTA at 5.

<sup>39</sup> IT Coalition at 3-4 n.7.

<sup>40</sup> PK/CU at 9.

and adopt the Jointly Proposed Robustness Rules.

## **II. Section 73.9006 of the Commission's Rules Must Be Corrected**

The Commission must also clarify Section 73.9006 to remove any possibility of confusion caused by an apparent formatting error introduced when the rule was edited for publication. As set forth in the Joint Proposal, and as drafted from April 2002 to November 2003, what is now Section 73.9006 was a single paragraph composed of two sentences:

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 . . . , it shall so pass such content (a) using a Robust Method; or (b) 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. *Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.*

The second sentence thus clarified the entire first sentence, and stated that no matter which method is used to protect Marked or Unscreened Content being passed by a computer add-in product, *in no event* is such content to be passed via a User Accessible Bus unless it is either encrypted or uncompressed.<sup>41</sup>

When Section 73.9006 was published, however, paragraph breaks were inserted before subsections (a) and (b), but not before the second sentence, leaving the second sentence grouped with subsection (b):

Where a covered demodulator product passes unscreened content or marked content to another product, other than where such covered demodulator product passes, or directs such content to be passed to an output . . . , it shall

---

<sup>41</sup> See MPAA Petition at 21. Thus, in the Joint Proposal, subsections X.6(a) and X.6(b) were both introduced by a single instance of the clause, "it shall so pass such content." Likewise, the second sentence repeated this phrase, stating that content "may be so passed." The "so passed" in the second sentence obviously referred, and still refers, to both (a) and (b), which are both prefaced by the immediately prior instance of "pass."

pass such content:

- (a) Using a robust method; or
- (b) Protected by an authorized digital output protection technology . . . in accordance with any applicable obligations established as a part of its approval pursuant to Sec. 73.9008. *Neither unscreened content nor marked content may be so passed in unencrypted, compressed form via a User Accessible Bus.*

The MPAA is not proposing any changes to the text of Section 73.9006 at all, but simply that a paragraph break be inserted before the second sentence, so that it is returned to its status as a separate sentence and not confusingly grouped with Section 73.9006(b).

There is no evidence that this change to Section 73.9006(b) was anything but a formatting error. The Commission never offered any reason for the change. None of the many comments, reply comments, and *ex parte* letters filed with the Commission proposed making the second sentence apply only to Section 73.9006(b). Now, however, some parties are claiming that intolerable burdens would be imposed by the rule as originally proposed. The IT Coalition claims that the section as originally drafted “would unnecessarily increase cost and stifle innovation designed to improve the efficiency and functionality of PC-based devices.”<sup>42</sup> The IT Coalition does not explain why, however, it must be allowed to pass unencrypted, compressed data over a User Accessible Bus, or why it waited almost two years to say so.<sup>43</sup> Indeed, the understanding of Section 73.9006 proposed by the IT Coalition makes little sense, since under the IT Coalition’s view, only Authorized Digital Output Protection Technologies would be prohibited from allowing unencrypted, compressed data to be passed via a User Accessible Bus, whereas Robust Methods,<sup>44</sup> which are subject to less supervision, would be free to do so. If the

---

<sup>42</sup> IT at 7.

<sup>43</sup> The IT Coalition suggests that authentication could be used as an alternative to encryption, but in fact authentication is meaningless without encryption. *See* IT at 7.

<sup>44</sup> *See supra* note 30.

second sentence applies to only one subsection, it should be subsection (a), not subsection (b).

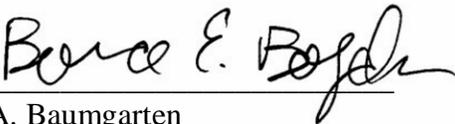
Like the IT Coalition, ATI Technologies also objects to returning Section 73.9006 to its former state, stating that to do so would “limit manufacturers to only one Robust Method.”<sup>45</sup> It is not at all clear what ATI Technologies means by “one Robust Method,” or even if it truly disagrees with MPAA on this issue. There are of course multiple means of designing Robust Methods; however, none of them must allow data that is *both* unencrypted *and* compressed to exist on a User Accessible Bus, because unencrypted, compressed data is too susceptible to interception. The Commission should reject these oppositions and return Section 73.9006 to its original meaning.

## **CONCLUSION**

For the reasons stated above, the Motion Picture Association of America, Inc., respectfully requests that the Commission amend its Broadcast Flag Order to adopt the Jointly Proposed Robustness Rules, and to clarify that Marked and Unscreened Content are not to be made available in unencrypted, compressed form via a User Accessible Bus.

Respectfully submitted,

MOTION PICTURE ASSOCIATION OF AMERICA, INC.

By: 

Jon A. Baumgarten

Bruce E. Boyden

Proskauer Rose LLP

1233 Twentieth Street NW, Suite 800

Washington, DC 20036

(202) 416-6800

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

---

<sup>45</sup> ATI at 5.

**CERTIFICATE OF SERVICE**

I, Bruce E. Boyden, hereby certify that a true and correct copy of the Omnibus Reply of the Motion Picture Association of America, Inc. to the Oppositions Filed by ATI Technologies, Inc., the Consumer Electronics Industry, the IT Coalition, the National Cable & Telecommunications Association, and Public Knowledge & Consumers Union was served on the following parties on March 22, 2004, by first-class mail, postage prepaid:

Geoff Phillips  
ATI Technologies, Inc.  
33 Commerce Valley Drive East  
Thornhill, Ontario L3T 7N6  
Canada

Michael D. Petricone  
Consumer Electronics Association  
2500 Wilson Boulevard  
Arlington, VA 22201

Marc A. Pearl  
Consumer Electronics Retailers Coalition  
1341 G Street NW, Suite 1100  
Washington, DC 20005

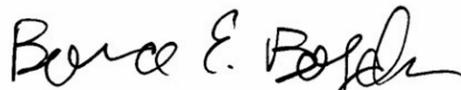
James M. Burger  
M. Anne Swanson  
Dow, Lohnes & Albertson PLLC  
1200 New Hampshire Ave. NW, Suite 800  
Washington, DC 20036  
*Counsel for the IT Coalition*

William A. Check, Ph.D.  
Andy Scott  
Daniel L. Brenner  
Neal M. Goldberg  
Loretta P. Polk  
National Cable & Telecommunications  
Association  
1724 Massachusetts Avenue NW  
Washington, DC 20036-1903

Paul Glist  
Cole, Raywid, & Braverman LLP  
1919 Pennsylvania Avenue NW, Suite 200  
Washington, DC 20006  
*Counsel for the National Cable &  
Telecommunications Association*

Nathan Mitchler  
Mike Godwin  
Public Knowledge  
1875 Connecticut Avenue NW  
Washington, DC 20009

Christopher Murray  
Consumers Union  
1666 Connecticut Avenue NW  
Washington, DC 20009



---

Bruce E. Boyden