

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

**In the Matter of** )  
 )  
**Digital Broadcast Content Protection** ) **MB Docket No. 02-230**  
 )

**OBJECTIONS TO THE “PETITION FOR RECONSIDERATION AND  
CLARIFICATION OF THE MOTION PICTURE ASSOCIATION OF AMERICA,  
INC”**

ATI Technologies, Inc. (“ATI”) hereby submits the following objections to the Petition for Reconsideration and Clarification filed by the Motion Picture Association of America, Inc. (“MPAA”) of the First Report and Order in the above captioned proceeding.<sup>1</sup>

ATI is a leading supplier of digital television demodulator and visual image processing products for the personal computer and consumer electronic industries. In addition to being one of the world’s largest computer graphics chip suppliers, it develops and sells add-in boards for the personal computer that allow consumers to watch and record analog television on the computer.

ATI applauds the Commission for balancing the burden on manufacturers, the cost to consumers, and the goals of Broadcast Protection in formulating the Robustness Requirements (§73.9007). ATI objects to the MPAA's Petition in so far as it asks the Commission to increase the level of robustness as defined in the Robustness Requirements above that of “ordinary users” thereby asking the Commission to reverse its robustness decision. ATI also objects to the MPAA’s request for “clarification” of §73.9006 whereby

---

<sup>1</sup> Digital Broadcast Content Protection, *Report and Order and Further Notice of Proposed Rule Making*, MB Docket No. 02-230 (rel. Nov. 4, 2003) (the “Broadcast Protection Order”)

the MPAA would have the Commission reverse its decision to permit the transfer to add-in covered demodulator products of compressed Unscreened and Unmarked Content protected by a Robust Method.

I. Raising the Level of Robustness Will Have Little Impact on Indiscriminate Distribution of DTV But Will Harm Manufacturers and Raise the Cost of Digital Television to Consumers

The MPAA claims that raising the level of robustness will cause manufacturers to “suffer no harm”.<sup>2</sup> ATI is one of those manufacturers, and it strongly disagrees with the motion picture studios’ claim.

A decision to increase the robustness level will require a demodulator to determine if a downstream device can be trusted.<sup>3</sup> To achieve the level of robustness advocated by the MPAA, determining trustworthiness can only be properly performed through a key exchange using public key cryptography.<sup>4</sup>

Public key cryptography between a demodulator and decoder device would require the demodulator and decoder manufacturers to agree to a common secure protocol, embed cryptographic technology and securely embed unique secrets into each device. Securely

---

<sup>2</sup> Petition for Reconsideration and Clarification of the Motion Picture Association of America, Inc., in MB Docket No. 02-230 (filed Jan. 2, 2004) (“MPAA Petition”) at 17.

<sup>3</sup> Our engineers are “experts.” While not normally possible for an ordinary user, our engineers know how to hack into the demodulator/decoder module to obtain the same video that was transmitted in the clear. To defend against an “expert” attack DTV demodulator silicon providers would have to put in some form of scrambling into the actual demodulator. A DTV demodulator silicon provider could use a fixed key, but that would be broken in short order so they would have to put in a mechanism for key management and exchange. This is the point where “security” gets difficult and expensive. (Tim Polk at NIST calls key management a “nightmare”. See, <http://www.cacr.math.uwaterloo.ca/conferences/1999/isw-march/polok.ppt>, last visited Mar. 10, 2004). Key management and exchange will increase the cost of both the demodulator and the decoder silicon. Furthermore, ATI’s key management and exchange mechanisms will most likely not be the same as a competitor’s key management and exchange mechanisms; therefore, a DTV manufacturer would most likely have to select a demodulator and a decoder from the same silicon provider to ensure demodulator and decoder interoperability. This effort is all for protecting something that was originally transmitted in the clear. It doesn’t make sense.

<sup>4</sup> See <http://www.rsasecurity.com/rsalabs/faq/2-1-1.html> (last visited Mar. 10, 2004) for a discussion on public key cryptography.

embedding unique secrets into each device will increase demodulator and decoder device cost significantly as it will require embedding non-volatile memory into each device.<sup>5</sup> Also, since there is no standard design for expert-level robustness, each manufacturer will have to develop their own design in an effort to meet this higher level of security.

In addition to the expense of securely embedding keys, and “one-off” security redesign, achieving this increased level of robustness will most likely require the demodulator and decoder to be designed and sold together.<sup>6</sup> This will severely affect, if not destroy, the existing market for demodulators currently sold for most high-end digital televisions and set-top boxes. It will add cost to DTV receivers. In general, high-end digital television and set-top box manufacturers purchase demodulators as part of an Integrated Tuner and Demodulator (“ITD”). The ITD is purchased from one manufacturer. Generally the decoder is purchased from another manufacturer. Before robustness is raised to an unnecessary high level, the increased expense of integrating the demodulator and decoder, in an effort to thwart an expert, must be balanced against both the destruction of the legacy demodulator market and the increased cost and burden to receiver manufacturers.

It is well accepted that hackers will attack the weakest link in a system. Accordingly, increasing the robustness level and the cost of DTV products will have no effect on hackers.

The ATSC demodulator specifications are publicly available, and DTV will continue to be

---

<sup>5</sup> Non-volatile memory can be embedded by integrating a separate EEPROM or flash device in the same package as the device silicon. That method will increase cost of a device because the manufacturer would have to include the cost of the non-volatile memory. In addition, it would most likely lower production yields, thus, increasing the overall cost of the device. An alternative solution would be to integrate an EEPROM or flash memory into the same silicon die as the demodulator or decoder. This method would increase the surface area of the silicon which increases costs. This method might also require the silicon manufacturer to change or modify their fabrication process. Not only would this affect the silicon cost but it would also increase a manufacturer’s time to market and most likely lower production yields.

<sup>6</sup> See note 3 supra.

transmitted in the clear. Therefore, any “expert” or technically inclined person could simply build their own demodulator that would ignore the broadcast flag.<sup>7</sup> The GNU Radio Project already provides any “expert” or technically inclined person with working source code for developing such a device on a personal computer.<sup>8</sup> Expert-level device robustness, therefore, will impose unreasonable costs on the system for little or no return.

Finally, robustness rules must match system goals. As the Commission noted:

MPAA advocates adoption of the ATSC flag system and characterizes it as an effective and unobtrusive content protection mechanism that will serve as a “speed bump” to ensure that DTV broadcast content is not indiscriminately redistributed.<sup>9</sup>

Indeed, throughout the order, the FCC characterizes the flag system as a “speed bump.”<sup>10</sup> As noted above, and in footnote 7 above, there are a variety of other roads through which DTV content may escape to be indiscriminately redistributed. Most of those, except legacy receivers, require relatively low level of technical expertise which is in and of itself a speed bump. But the MPAA would have one road, that of commercial DTV products, be barred not by a speed bump, but by a wall. This is simply inconsistent with DTV system technology and the Commission’s goals. Accordingly, the Robustness Requirements should not be changed.

---

<sup>7</sup> In addition, by the end of this year, consumers will own a large number of unprotected legacy receivers permitting “hacking by eBay,” i.e., purchase of an unprotected receiver. Moreover, as appears to be the case with indiscriminate Internet redistribution of movies, leakage of content before it gets to the transmitter will likely be a far greater source of DTV material on the Internet than any expert hack of a covered demodulator product. Thus, despite the hack of DVD CSS, the vast majority of video content on the Internet appears to come from leaks in the distribution chain from studio to theater. The same is likely to be true for protected DTV content, i.e., leakage from TV production to transmitter. Finally, there is the so-called “analog hole” through which DTV content will leak. See Broadcast Protection Order at ¶19.

<sup>8</sup> See “GNU Radio—The GNU Software Defined Radio,” <http://www.gnu.org/software/gnuradio/gnuradio.html> (last visited Mar. 10, 2004). See also Eric Blossom, “GNU Radio: A Free Software Defined Radio,” presentation to the Copy Protection Technical Working Group, February 27, 2002, <http://www.cptwg.org/Assets/Presentations/gnuradio-27-feb-2002-cptwg.ppt> (last visited Mar. 10, 2004). The current GNU Radio source code, in C++, is available by anonymous CVS from: [pserver:anoncvs@subversions.gnu.org:/cvsroot/gnuradio](mailto:pserver:anoncvs@subversions.gnu.org:/cvsroot/gnuradio).

<sup>9</sup> Broadcast Protection Order ¶ 14.

<sup>10</sup> See, e.g., *Id.* at ¶¶ 19 and 20.

II. The MPAA's "Clarification" for Add-in Computer Products is a Substantial Change and Should Be Denied

Section II of the MPAA's Petition asks for clarification of the obligation of add-in computer products manufacturers using Robust Method transfers to ensure that compressed Marked and Unscreened Content is not available in unencrypted form via a User Accessible Bus. We do not disagree with the MPAA's statement that compressed content carried over a User Accessible Bus is "susceptible to being intercepted and should never be present where it can be easily accessed." We part company with the MPAA, however, when it concludes that the Commission incorrectly wrote §73.9006 and:

... that no outputs for computer add-in products should be allowed to expose unencrypted, compressed data over a User Accessible Bus, whether protected by an Authorized Digital Output Protection Technology or by a Robust Method.

The MPAA's conclusion conflicts with its first statement. Use of a Robust Method, by definition, must prevent a user from easily accessing unencrypted, compressed content wherever the content resides. The Commission was correct; there is no basis for changing the rule to limit manufacturers to only one Robust Method.

The User Accessible Bus definition was written several years ago, but technology has advanced.<sup>11</sup> Most modern computer video add-in cards employ a *point-to-point connection* like an Advanced Graphics Port ("AGP") interface or, starting in the spring of 2004, a Peripheral Component Interconnect Express ("PCIE") interface to connect to the computer as opposed to a *bus* where multiple devices may be connected and all devices on the bus can record communication on the bus.<sup>12</sup> The new PCIE point-to-point connection, while user accessible, is technically part of the internal architecture of a computer and are as secure and

---

<sup>11</sup> The term "user accessible bus" appears to have been first employed in the 1997 DVD CCA CSS Interim Procedural Specifications. Seven years (or over 4.5 Moore's Law cycles) is a long time in PC product development.

<sup>12</sup> An example is the old Peripheral Component Interconnect ("PCI") bus.

robust as memory buses or CPU interface buses.<sup>13</sup> It would be extremely difficult for an ordinary user and difficult for an expert to record Marked or Unscreened Content carried on the PCIE connection even with expert tools. Thus, the “clarification” proposed by the MPAA is actually a substantial change to the rules.

It is clear that the intent of the User Accessible Bus language is that if an ordinary user could otherwise gain access to compressed Unscreened or Marked Content in useable form, the obligation is to use a Robust Method to protect such content. The Commission wrote the rule exactly right. Requiring any one particular method will not provide any additional protection. Instead, it will only serve to increase the cost to consumers and chill innovation. We urge the Commission not to change the current wording in §73.9006 – Add-in Covered Demodulator Products.

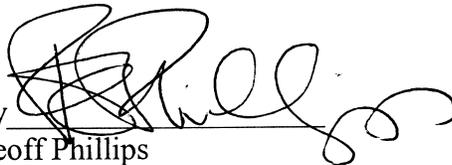
---

<sup>13</sup> Memory buses are routinely accessed by users to upgrade their PCs.

Therefore, ATI respectfully requests that the Commission reject the MPAA's Petition for Reconsideration and Clarification in so far as it would reverse the Commission's rules on the level of robustness and protection of compressed content using a Robust Method.

Respectfully submitted,

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

By 

Geoff Phillips  
Vice-President and General Manager  
DTV Business Unit  
Consumer Products Division  
ATI Technologies, Inc.

March 10, 2004