A Promising Future: Content Protection and Anti-Piracy

By Jim C. Williams, Krishnan Rajagopalan, and Robert Bauer
Motion Picture Association of America (MPAA)

Introduction

This progress report provides the current status of content protection and anti-piracy and describes key challenges for the near-term future. Content protection and anti-piracy are both measures to protect the "residual value" of movies and television in each stage of their respective distribution channels. Content protection strives to contain leaks from legitimate distribution channels through the use of technological measures. Anti-piracy, likewise, strives to contain leaks, but also endeavors to thwart illegitimate distribution channels through use of technological, physical, and legal enforcement measures.

Context of Rapid Transition and Change

For years, and in some cases decades, movies and television have been undergoing a well-hyped transition from analog to digital, as depicted in Fig. 1.

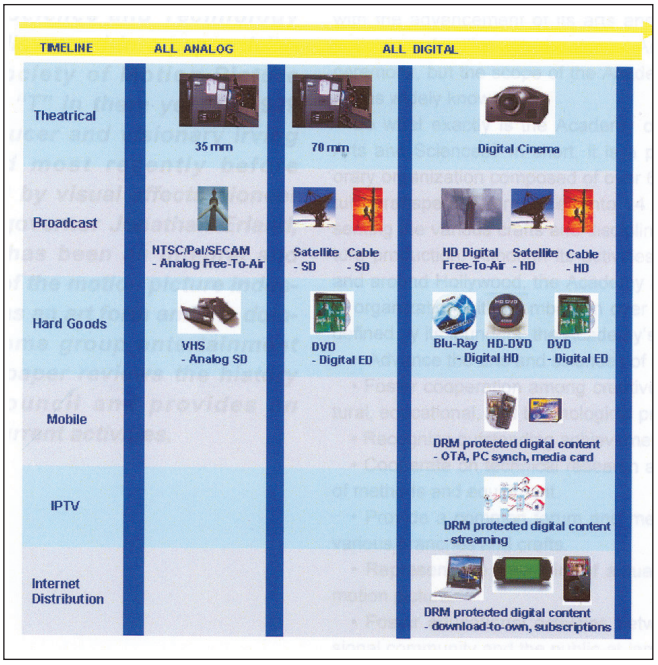


Figure 1. Trends: Analog to Digital

In addition to the transition to digital technologies, there is currently a steady push for a transition to more interoperable solutions providing portability of devices around the world between regions, as well as the portability of content between consumer devices, as depicted in Fig. 2.

The digital transition and move toward greater interoperability provide incredible opportunities for content providers, among others, to offer content in new and exciting ways. The mantra of the modern consumer is "what I want, where I want it, when I want it and on whichever device I happen to be carrying or sitting in front of." Film studios and television broadcasters are highly motivated to meet the dynamic demands of the enter-

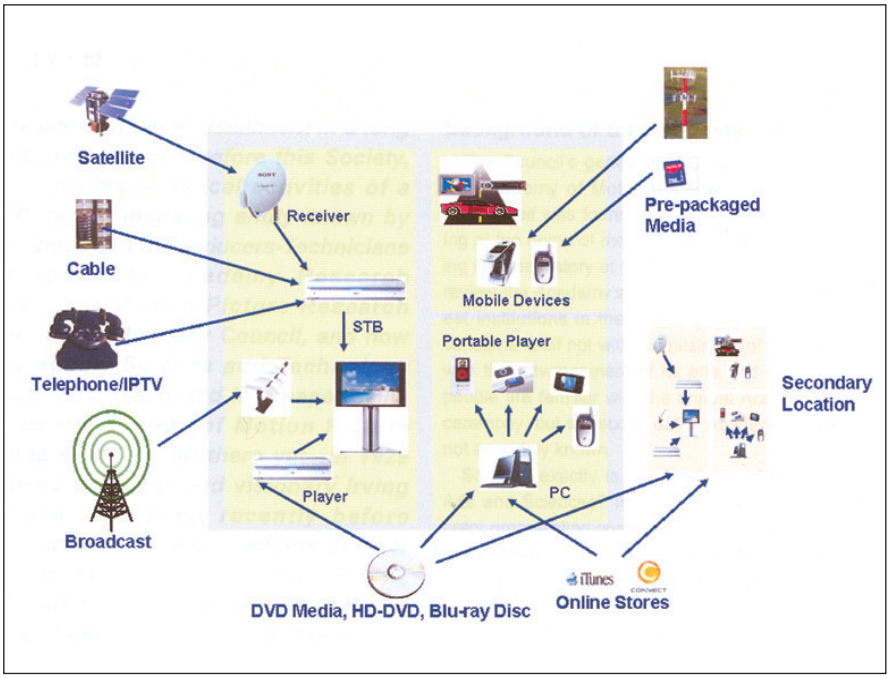


Figure 2. Trends: One to Many to All Interoperable.

tainment consuming public—an increasingly large, disparate, and demanding audience.

Studios are racing to the marketplace with exciting new products, but are doing so in a way that respects the balance of rights held by the content creator, content owner, and everyone in between. The role of content protection and anti-piracy is to illuminate a path for consumers to find safe, legal alternatives to find the entertainment content they are looking for, while providing an attractive alternative to dark back alleys of both our physical cities and cyberspace.

In order to be able to continue investing huge sums in moviemaking, the movie industry must be able to maximize revenue from each distribution channel while retaining residual value of the product for subsequent distribution channels. Piracy blurs the distinction between these lines.

Every participant in the movie and television distribution chain has an important role to play in maintaining the long-term health of the industry. Unless the transition to digital television is accompanied by diligent end-to-end adherence to content protection standards, the residual value of the content will evaporate into the ether, or more specifically, the internet.

Content Protection

Traditional content protection over the past several years has included CSS protection for DVDs, Conditional Access for cable and satellite, and copy protection for analog outputs. The following sections discuss content protection trends in these areas.

Packaged Media Content Protection Trends (CSS to AACS)

For years the Content Scramble System (CSS) for protecting DVDs has been technically broken. Its secrets were published and De-CSS programs sprang up to exploit the technological weakness. Through enforcement efforts these programs have been pushed to the back alleys and away from the legitimate storefronts.

CSS provides an example of the importance of the content protection system license. Such licenses include compliance and robustness rules that dictate the obligations of all legitimate manufacturers of chips and devices that decrypt and decode the protected content.

Even though the technological protections are severely damaged for CSS, the license is sound and able to support the continued importance of DVDs as a key distribution mechanism for movies and, more recently, TV episodes.

In recent years, the DVD CSS Procedural Specifications, i.e., the license, has been amended to include three different digital content protection systems as approved outputs of DVD players:

1. High-bandwidth Digital Content Protection (HDCP) for DVI and HDMI interfaces (in 2003).
2. Digital Transmission Content Protection over Internet Protocol (DTCP-IP) for wired and wireless Ethernet (in 2004).
3. Windows Media DRM for Networked Devices (WMDRM-ND) for wired and wireless Ethernet (in 2005).

Recent public reports have suggested that even further improvements are under consideration for the traditional DVD.

In May 2006, Toshiba began distribution in the United States of their HD DVD players. Blu-ray Disc players are expected soon and will likely be available in the U.S. by the time this report is published. Both systems use the Advanced Access Content System (AACS), which includes, as CSS, both technological and license components to its protection. AACS published an interim license in February 2006.

On the technological side, AACS includes the following key attributes that should make it significantly more reliable in the long-term than its predecessor:

- AES-128 content scrambling
- Media Key Block-based revocation
- Software renewability
- Enhanced authentication for PC-based implementations
- Support for managed copying and download-to-burn usage models

The Blu-ray Disc format adds a few more technological methods to enhance renewability and forensic monitoring.

On the license side, AACS includes the following important attributes:

- Inclusion of Copy Generation Management System for Analog (CGMS-A) copy control and RC redistribution control signaling on all analog outputs.
- Designation of the Verance audio watermark for

playback control using two marks: "consumer use" and "theatrical no home use."

• Approval of the same three digital outputs that are approved for DVD players.

• Processing of the Image Constraint Token, if signaled, to down-resolve content being output to unprotected high-definition analog outputs.

• Processing of the Digital Output Only Token, if signaled, to turn off analog video outputs.

• Sunset of high-definition analog outputs after 2011.

• Sunset of all analog outputs after 2013.

AACS provides a common content protection framework in the midst of the HD DVD and Blu-ray Disc format war.

Conditional Access Trends (Footprint to DRM)

The original conditional access was simply living within a terrestrial broadcast footprint—a family could only access that broadcast upon condition of being within the broadcast transmission footprint. Traditional analog cable can only be accessed on condition of having the cable from the street connected to the cable entering one's home.

Riding on the digital transition, satellite, cable, and, in a few special cases, terrestrial broadcasters began using full-featured, digital encryption-based, Conditional Access (CA) systems from such companies as News Digital Systems, Nagravision, Irdeto Access, Motorola, Scientific Atlanta, Conax, and Viaccess, among others. With the recently reinvigorated push from the world's telephone companies to complete the "triple play" of voice, data, and video, additional companies have joined the competition for the security of the delivery platform, including Microsoft, Widevine and others. Content is also being delivered via the World Wide Web over cable, DSL or fiber-to-the-home broadband internet connections. The security for delivery of these systems is provided by Digital Rights Management (DRM) systems, from companies like Microsoft and Real. Such systems ensure that the business rules established by the content provider are enforced, e.g., if a family pays for a package of 150 channels, then they get access to those channels on a certain number of set-top boxes in the home to which the bills are sent.

Conditional Access systems have been heavily hacked in recent years, and most systems have undergone renewal or replacement. Renewal is performed through smartcard replacement, software download, or both. There is a heavy motivation among CA providers and the PayTV providers to ensure the integrity of this system and they have very proprietary and sensitive plans and activities in place to achieve this goal.

Recent technological thrusts in CA and DRM have been motivated by two key desires:

• Portability of the PayTV receiving device from one service provider to another.

• Ease of transition by a service provider from one CA provider to another.

A more challenging problem exists for Clear-To-Air, or unencrypted, transmission of Free-To-Air, typically terrestrial, television. With broadband internet connections, one can no longer rely on the broadcast footprint to contain leakage into other markets. The measures being taken to address this problem are explored below.

Copy Protection Trends (Nil to Home Networking and Remote Access)

The original copy protection was lack of recording devices. With the advent of the VCR, systems such as Macrovision were used to degrade recording of content for which no right to record was granted. Later, Dwight Cavendish provided a competitive alternative.

Today, it is commonplace for video outputs of devices that play movies (DVD players) or decode TV (set-top boxes) to include Copy Generation Management System for Analog (CGMS-A) signals in the vertical blanking interval. Standards exist for NTSC, PAL, SECAM, 525p, 625p, 720p, and 1080i video signals. The CGMS-A signals provide the ability to signal "copy never," "copy once/copy one generation," "copy no more," and "copy control not asserted." Recording devices, e.g., DVD+RW recorders, look at these signals to determine whether or not they can make a recording of an incoming signal. Some of the standards have been recently updated to include redistribution control information to signal whether or not such content can be redistributed over the internet.

Copying is no longer the only desire of the consumer. They wish to move content around their home, onto a personal video recorder, to the bedroom, to a recordable DVD, to the car, to portable devices, and even to remotely access from their hotel room while on the road. The term "copy protection" is a little overwhelmed in the face of these usage models.

To address the pent-up demand for richer user experiences when consuming content, significant development resources have been expended in the last few years to define an interoperable digital home networking infrastructure that is suitable for movies and television. The work of Digital Living Network Alliance (DLNA) for Ethernet-based networks and High-definition Audio-visual Network Alliance (HANA) for 1394/Firewire-based networks is noteworthy. These systems have the ability to do much more than allow a set-top box to access content or to allow an output to be recorded onto a piece of physical media. These solutions offer the Holy Grail of Anywhere, Anytime, Anyone, Any Device through promised and highly sought-after digital interoperability.

To ensure that such systems are used in accordance with content usage rights granted by the content owner and conveyed through the distribution chain, a much more sophisticated form of copy protection is needed. We use the term Content Protection and Copy Management (CPCM) for such systems. This refers to a system that can determine content usage rules that are associated with content upon acquisition (e.g., reception as free-to-air, access from a CA system, access from a DRM system, or output from a packaged media content protection system) and securely manage the content in accordance with those rules until consumption. This type of system, overlaid on top of DLNA or HANA, can enable the use of such interoperable systems for commercial content such as movies and TV. An example of a standardized CPCM is nearing completion by the Digital Video Broadcasting (DVB) consortium. The DVB Blue Book A094 includes the first three parts of this specification and can be downloaded for free from www.dvb.org. Other proprietary content protection systems that could be used as a CPCM include Secure Video Processor (SVP) and Windows Media DRM, among others.

As a precursor to a feature-rich CPCM content protection mechanism that offers persistent protection, several link protection technologies have been developed and are currently available for use. These link protection schemes provide technology to secure content during transmission from one device to another and rely on license terms to protect the content inside the source and sink devices.

To further understand link protection systems, we suggest reviewing the two different link protection systems that are approved as digital networking outputs of DVD players, Digital Transmission Content Protection over Internet Protocol (DTCP-IP) and Windows Media DRM for Networked Devices (WMDRM-ND, a.k.a. Cardia). In addition, HDCP is a commonly used link protection scheme for high-definition digital connections.

Internet and Mobile Trends

In addition to the digital transition in the broadcast world, the explosive growth of broadband internet and mobile phones has enabled a number of new distribution models over IP networks. Almost 70% of users in the U.S., for example, have broadband access to the internet. Of the 17% of teens (age 13-17) who have mobile phones, 57% have data plans (source: Nielsen/NetRatings). In many countries, e.g., South Korea and Japan, the numbers are significantly higher.

Internet

On the internet front, the popularity of services like iTunes is driving the market for digital consumption of audiovisual content on PCs and portable devices using download-to-own (users buy a specific title), rentals, and subscriptions (users pay for the right to watch unlimited content in a given time-period) business models. Content delivered through these services is protected by DRM technologies, which typically bind the content to a set of devices that are identified with a specific user. The user typically consumes the content on a set of authorized PCs and also a set of portable video players that are registered with the authorized PCs. Common DRM technologies in the market are Apple's Fairplay, Microsoft's WMDRM, Sony's OMG, and Real Helix DRM.

Mobile

On the mobile front, wireless operators are also offering different mechanisms to consume audiovisual content that is protected using DRM technologies on mobile phones. Content is delivered to mobile phones using PC-synchronization, OTA (over-the-air) downloads and OTA streaming technologies. In addition, broadcast standards such as DVB-H also provide direct access to broadcast content on mobile devices. Content acquired from mobile operators can typically be consumed only on a specific mobile device. Common DRM technologies in the mobile space include CMLA's OMA and WMDRM.

Challenges for Content Protection

Unencrypted Digital Broadcasts (Broadcast Flag)

Today, free-to-air broadcast television is under attack from internet thieves. TV is licensed for transmission in each individual region. However, in the digital world, the internet provides a lossless, unlimited redistribution vehicle throughout the world. For free over-the-air broadcasting to remain a viable means of distribution, the transition to digital television must be accompanied by a solution to prevent its unauthorized redistribution over the internet.

Audiovisual content rights holders are more likely to make their works available when they are adequately protected against illegal reproduction and retransmission. Technological solutions exist for all types of broadcasting systems, including ATSC, DVB, and ISDB-based systems, but government action is needed to be sure such solutions are applied and take effect. Governments throughout the world should embrace redistribution control for unencrypted digital transmissions as a necessary and narrow solution to safeguard the same interests that copyright rules protect, namely incentives to create, produce, and distribute quality audiovisual content.

The Broadcast Flag rule in the U.S. was defined for precisely this problem. In Europe, the European Broadcasting Union (EBU) is instrumental in advocating a DVB-based solution and DVB CPCM is a leading contender for protection of such broadcasts after reception. In the Asia-Pacific region, the Asia-Pacific Broadcasting Union (ABU) is instrumental in advocating appropriate solutions for the ATSC, DVB, and ISDB systems used within that region. In fact, Japan has already resolved this problem by using an encryption-based ISDB solution and a variety of content protection systems for the digital outputs of the ISDB receivers.

Analog Outputs to Support Older, Legacy Devices (Analog Hole)

Consumer products are migrating toward the use of "secure digital connections." Yet, analog connections will remain in use for many years to come to support older, "legacy analog devices." The problem facing the industry is that analog connections can be redigitized, stripping the rights, and be subjected to unlimited copying and unauthorized redistribution over the internet. The solution is to require (i) rights signaling on analog audiovisual outputs and (ii) rights honoring by devices that can redigitize those analog audiovisual connections. This legislative and technological solution addresses these important requirements: (a) consumers need consistency of user experience; (b) consumers want more choices as to how to enjoy content and content owners need to know that the distinctions among various offerings will be respected; (c) manufacturers need a level competitive playing field; and (d) content owners need respect of copyright. By implementing this well-crafted and narrowly defined solution, the new digital market can thrive while relying upon analog to provide audiovisual interconnection to legacy devices without being used as a back door for theft.

DRM Interoperability

One of the key issues with the proliferation of these new distribution models is that content owned by the same user is now protected using different DRM technologies and Conditional Access systems which do not operate together in a symbiotic fashion. This creates an artificial barrier to how users can consume content in their homes. It is a significant challenge as home networks become more common. The next generation of home networks not only attempts to create a common IP network to share data between devices in the home, but also attempts to bridge the gap between the living room (traditional broadcast content destination), the study (typical internet con-

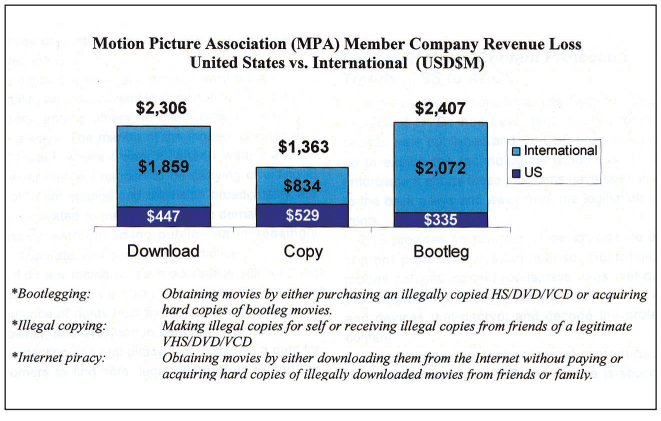
tent destination), and also outside the home (mobile content as well as managed remote access to content in one's home). Key standards bodies like Digital Living Network Alliance (DLNA, www.dlna.org), Digital Video Broadcasting (DVB, www.dvb.org), and Coral Consortium (Coral, http://www.coral-interop.org) are defining the secure home network of the future where users can consume content on any authorized device (irrespective of the DRM technology on the device), subject to the usage rights associated with the content.

Anti-Piracy

Impact of Piracy

In May 2006, the Motion Picture Association of America, Inc. (MPAA) released a comprehensive new study about the impact of piracy done by the LEK Consulting Group. According to the study, MPAA member company studios lost $6.1 billion to piracy in 2005, which is consistent with a piracy study conducted by Smith Barney in 2003 that predicted the motion picture industry would lose $5.4 billion to piracy in 2005. This immense loss is only the impact to studios. Every other participant in the movie and TV value chain is also greatly affected.

Of the $6.1 billion in lost revenue to the studios, $1.3 billion came from piracy in the U.S. and $4.8 billion internationally, with nearly half of that loss occurring in Europe. About $2.4 billion was lost to bootlegging,* $1.4 to illegal copying,* and $2.3 billion to internet piracy.* In the U.S., illegal copying and distribution is more of a problem, while internationally, illegal downloading and bootlegging is more prevalent.



Enterprising studios, however, are not looking at the results of this study as a jeremiad on the past, but as an opportunity to realize more profits in the future, this study being an indicator of unrealized revenue potential.

Multipronged Solution to the Piracy Problem

At home and abroad, online and in the streets, the MPAA and MPA have been successfully attacking the problem of piracy through a multipronged approach of education, technology, enforcement, and litigation. Any successful anti-piracy program aims to genuinely impact the experience of content consumers, to patrol a safer superhighway to reach the clean, safe zones, post road signs so no one gets lost, and to make known the benefits and availability of the safer superhighway . . . while at the same time making the backalleys harder to find, scarce, and less appealing to the majority of the moviegoing public.

Tactics employed to achieve our anti-piracy goals include a combination of education, traditional intelligence gathering, and forensic analysis along with new, innovative solutions, litigation and legislation, as well as enabling new legitimate alternatives to piracy and theft of content.

Education

The MPAA is working to curb piracy through several influential education initiatives such as collaborating with "Weekly Reader" and a leading internet safety educator, "Wired Safety," among others, for example:

• November 2005: MPAA launches a public service announcement contest for college students in partnership with Students in Free Enterprise.

• April 2006: MPAA and Weekly Reader launch a new education program to inform parents, educators, and students about internet safety.

• April 2006: MPAA and RIAA launch systematic program to identify and curtail campus Local Area Network (LAN) piracy at universities across the country by alerting 40 university presidents in 25 states of LAN system abuse.

Intelligence-Based Enforcement

Every disc and digital file tells a story. Using state-

of-the-art forensics, we unlock a library of data critical to solving cases and producing investigative results. For every hard disc gathered and digital file tracked, a wealth of evidence is collected about its source, destination, method of delivery/transshipment, and other characteristics. Microscopes in our forensics laboratory capture evidence necessary to link any replicated disc to the precise replication machine that made it.

Using a combination of digitally imbedded markings and advanced forensics, we are now able to reveal the original source, with startling accuracy, of any piece of any stolen film. For example, from examining a single scene on a movie purchased on the streets of Brazil, we can determine the precise address of the theater in the U.S. where the video track was camcorded and the telephone number of the theater in Mexico City where the Spanish-language audio track was lifted before the two tracks were combined online. We can determine the name of the Academy award voter whose grandson "borrowed" the screener and posted it to the latest P2P system, and the editing vendor where an employee thought he could get away with lifting one disc and sharing that with a friend.

Intelligence gathered worldwide from these forensic analyses is then fed back to the MPAA's home office, analyzed for trends and links between sophisticated pirate networks, and disseminated back to any of our 62 local offices. As patterns emerge, we shift our enforcement efforts accordingly.

Innovative Tactics

As criminals grow more entrepreneurial in their approach to breaking the law, anti-piracy forces must remain vigilant in their approach to stopping them. Among these new practices, MPA anti-piracy experts currently employ DVD-sniffing dogs and undercover internet informers.

In May 2005, MPA successfully concluded a feasibility study, which determined that the same techniques used to train dogs to sniff and detect bombs, agricultural products, and more can be employed to teach dogs how to detect polycarbonate DVDs. After eight months of training, two black Labradors (named Lucky and Flo) were put to the test working with Her Majesty's Revenue and Customs in the U.K. and Fed-Ex. After a field test at London's Stansted airport, the dogs retrieved discs deeply hidden in packages not known to contain polycarbonate material. The results of this "outside the box" thinking on developing new enforcement tactics are to provide customs officials around the world with new tools to spot contraband at a cost-effective price. The MPA is currently accepting applications for venues and dates for the "Lucky and Flo World Tour" to demonstrate to customs officials worldwide, the possibilities.

Just as law enforcement relies on undercover informants to provide background and intelligence about criminal networks involved with drugs and other organized crimes, the MPA employs a team of expert internet investigators who deal regularly with informants online. As pirates run from the street into the virtual "dark alleys" of the internet, MPA anti-piracy forces are equipped to follow them.

How Have We Done?

Working with law enforcement around the world in 2005, MPA anti-piracy investigators initiated almost 79,000 cases that resulted in the seizure of over 82 million illegally pirated discs worldwide. 31,000 legal cases were initiated; 11,500 favorable court decisions were obtained (a majority of the remaining cases are still pending). And, perhaps most importantly, we can quantify a measurable impact on the criminal-consumer experience: sites that are well-known "home bases" for piracy such as eDonkey servers, DirectConnect hubs, Torrent-trackers, and a variety of facilitating websites. An increasing number of websites started to require user registration. As a result of increased pressure from law enforcement spurred on by the MPA, a majority of eDonkey servers once hosted in the U.S. have either closed or migrated to Europe. Of the 22 Torrent-tracker sites targeted within 3 rounds of lawsuits, 17 have closed and remained closed.

The MPAA has been working with law enforcement agencies worldwide in cracking down on copyright theft.

• February 2006: Belgian and Swiss authorities shut down Razorback2, the number-one eDonkey peer-to-peer server facilitating the illegal file swapping of approximately 1.3 million users simultaneously.

• February 2006: Crackdown on highly trafficked Torrent, eDonkey, and News Group sites responsible for illegal swapping by millions of users around the world. They provide a massive directory of illegal content to users and encourage people to traffic in copyrighted motion pictures, televisions shows, music, software, and games.

• March 2006: MPAA collaborates with the National Association of Theater Owners and Canadian associations to launch online training program www.FightFilmTheft.org in U.S. and Canada to combat illegal camcording in movie theaters.

Providing Legitimate Alternatives to Piracy and Theft

An important part of addressing piracy is ensuring that there are ample legitimate alternatives to address demand. Accordingly, studios and networks are expanding their distribution channels to harness new technologies to deliver content in a variety of new ways. New ventures and offers are being announced in rapid fire succession. These are a sampling:

• Warner Brothers partners with Free Record Shop using P2P distribution

• Universal partners with LoveFilm in U.K., offering downloads

• CBS and Verizon FiOS TV partner to carry select programs

• Disney offers feature-length film on ITunes

• CBS delivers college basketball “March Madness” online

• ABC offers free downloads at ABC.com

• Disney re-launches MovieBeam—online delivery of VOD

• NBC Universal launches Aeon Digital set-top box

• CBS offers select programs on demand

• Warner Bros. launches P2P service In2Movies in Germany

• Fox announces VOD and DVD windows collapsed

• NBC Universal announces Peer Impact deal

• Disney announces deal with iTunes

• Google Video beta launched—essentially is going with a wholesale reseller model—creating an iTunes-like store.

Litigation and Legislation (Anti-Piracy)

The final prongs of the content protection and anti-piracy efforts address litigation and legislation. The MPAA continues to see important successes in these areas that are vital to the health of the motion picture industry moving forward. Recent highlights include:

• 2005/6: Six injunctions against DVD chip manufacturers, requiring that they abide by the terms of the DVD CSS License.

• April 2005: President signs Family Entertainment and Copyright Act of 2005, making camcording in theaters a federal felony.

• June 2005: Supreme Court in MGM vs. Grokster unanimously rules against online networks that encourage illegal distribution of copyrighted files.

• January 2006: International motion picture pirate leader Randolph Hobson Guthrie III pleads guilty in a Mississippi federal court to conspiracy to traffic in counterfeit goods, forfeiting $800,000 to the U.S. government.

• May 2006: Bill introduced in Senate Commerce Committee to protect broadcast content from piracy.

Conclusion

The content protection and anti-piracy measures described herein are directed toward providing as safe an experience as possible—indeed, as is demanded—for studios to sell their products to the public. There will always be those who attempt to game the system to get something for nothing or get more for less. The measures described herein are directed toward driving these pirates into the dimly-lit back alleys, both literally and in cyberspace, where criminals belong.

The Authors

This paper was co-authored by the following three executives from the Motion Picture Association of America, Inc.:

Jim C. Williams—Vice-President, Television & Video Systems Standards

Krishnan Rajagopalan—Vice-President, Digital Media Technologies

Robert Bauer—Director of Special Projects, Worldwide Anti-Piracy.