MOTION PICTURE ASSOCIATION
OF AMERICA, INC.
1600 EYE STREET, NORTHWEST
WASHINGTON, D.C. 20006
(202) 293-1966
FAX: (202) 293-7674

FRITZ E. ATTAWAY
EXECUTIVE VICE PRESIDENT
SPECIAL POLICY ADVISOR

March 16, 2007

VIA E-MAIL

Mary Rasenberger
Director of Program Management
National Digital Information Infrastructure and Preservation Program
Office of Strategic Initiatives
Library of Congress
James Madison Memorial Building
LM-637
101 Independence Avenue, SE
Washington, D.C. 20540

Re: Written Comments Relating to the Copyright Office's 108 Study Group Copyright Exceptions for Libraries and Archives

This is in response to the Federal Register Notice published by the Copyright Office on December 4, 2006, concerning the above-captioned matter. Motion Picture Association of America (MPAA) is a trade association representing six of the largest producers and distributors of feature films, home video material and television programs. MPAA members are Buena Vista Pictures Distribution (The Walt Disney Company), NBC Universal, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation and Warner Bros. Entertainment Inc.

MPAA member companies are major owners of copyrighted audiovisual works and have a significant interest in this proceeding.

MPAA as well as several of its member companies have participated in earlier roundtable discussions held by the Copyright Office and have filed written comments. These comments are intended to supplement the positions articulated in earlier roundtables and in written comments filed by MPAA on April 28, 2006.

The Notice requests comment on whether amendments of Section 108(d), (e) and (g) are warranted, whether the exclusions in subsection 108(i) should be relaxed or eliminated, and whether copies of unlicensed electronic works should be allowed in order to provide user access. In presenting these questions, the Notice observes that any changes in Section 198 must conform to the obligations of the United States under the Berne Convention to provide exceptions to exclusive copyrights only "in certain special cases" that do "not conflict with the normal exploitation of the work" and do not "unreasonably prejudice the legitimate interests" of rights owners.

The basic purpose of this inquiry is to determine whether changes to Section 108 are necessary to serve the purposes of that section in light of technological change, particularly the emergence of the digital environment in which most works can be fixed, reproduced and/or distributed in digital form. The Notice points out that:

> Many of the section 108 exceptions were put in place on the assumption that certain natural limitations, or inherent inefficiencies in making photocopies, would prevent the exceptions from unreasonably interfering with the market for the work. ... The question then is how to craft rules around digital copying and delivery to enable libraries and archives to service users efficiently, without opening up the exception in a way that could materially interfere with markets for copyrighted works just as subsections (d) and (e) were limited in 1976 by subsection (g) in order to avoid the potential for those exceptions to be used in a way that would cause material market harm.

This, indeed, is the seminal question. This inquiry is not confined to how the limitations on exclusive rights in Section 108 should be expanded to better enable libraries and archives to carry out the intent of that section in light of technological developments since 1976. Of equal importance to this proceeding is how Section 108 should be adjusted to maintain the carefully crafted balance between libraries and archives on one side of the equation, and rights holders on the other, in light of technological developments that can materially increase harm to rights holders resulting from the misuse of copies made under this section.

The digital revolution requires a reexamination of the Section 108 balance, whether or not non-text works are included in its limitations. Digitized text works can be easily reproduced and distributed literally around the world in seconds on the Internet. This fact should place a greater burden on libraries and archives to insure that works reproduced and distributed pursuant to Section 108 are restricted to scholarly purposes as distinguished from entertainment purposes. The nebulous term "private study" should not be used as a standard under Section 108, or if it is, it must be precisely and narrowly defined. An inappropriately defined "private study" standard would invite abuses, especially if entertainment works like movies, videos and TV show are included within the Section 108 limitations.

At least for some text works, like books, most people still prefer a bound copy acquired from the publisher to an electronic copy or a paper copy printed from an electronic copy. This is not the case for other types of works, most particularly movies, videos and TV shows, where a digital copy is incresasingly the preferred manner of consumption. Thus, extra care must be given to whether these types of works are made subject to the Section 108 limitations. If they are, uses must be strictly limited to scholarly purposes with effective safeguards to prevent abuse.

As owners of audiovisual entertainment material, the threshold issue for MPAA member companies is Topic B in the Notice: "Should subsection 108(i) be amended to expand the application of subsections (d) and (e) to any non-text-based works, or to any text-

based works that incorporate musical or audiovisual works." Obviously, if this question is answered in the affirmative with respect to movies, home videos and TV programs, Topic A questions also become relevant.

MPAA is not opposed in principle to expanding Section 108 limitations to audiovisual works, so long as it is done in a way that maintains the carefully crafted balance and does not interfere with normal exploitation. An examination of whether Section 108 should be expanded to cover audiovisual works should first consider the nature of particular audiovisual works. In the case of movies, home videos and TV programs, which are widely available and are principally of entertainment value, there is a real question as to whether these works should be subject to the Section 108 limitations at all.

It is worth noting that Section 108(d) does not distinguish between works that are readily available and those that are not. None of the Section 108 limitations are restricted to "orphan" works where the owner cannot be determined, and which are the subject of another on-going discussion. If Section 108(d) is expanded to cover non-text works, especially entertainment works like movies, videos and TV shows, it may be appropriate to restrict that subsection, as does Section 108(e), to works that cannot be readily obtained in the marketplace.

If Section 108 is expanded to cover audiovisual works, it is imperative that any digital reproduction or distribution be conditioned on application of effective technological measures that identify the source of the material and prevent wholesale copying and redistribution. The balance sought by Section 108 and our international obligations cannot be maintained if normal exploitation of works subject to the limitations is cut short by uploading them to the Internet for indiscriminate redistribution around the world.

Technology to discourage such indiscriminate redistribution is widely used and available in the marketplace. Watermarks in particular are an effective tool to identify the source of digital

material. (See attached White Paper on digital watermark technologies.) Whether or not Section 108 is expanded to cover non-text works, Section 108(g) should be updated for the digital age. Section 108(g) should specifically require the application of effective technical measures designed to prevent uses beyond "the isolated and unrelated reproduction or distribution of a single copy or phonorecord of the same material on separate occasions." At minimum, libraries and archives that take advantage of the Section 108 limitations to make digital copies should be required to incorporate a watermark that identifies the source of the works that are reproduced and distributed. This will provide an important incentive to libraries and archives, as well as to users, to take steps to ensure that the Section 108 limitations are not abused.

It should be noted that the Section 108 limitations do not limit the protections afforded copyright owners under Section 1201. That is, Section 108 does not permit libraries and archives to circumvent technical protection measures that prevent copying and redistribution. Thus, any Section 1201 issues are beyond the scope of this proceeding. Moreover, should section 108 be expanded to permit copies, in defined circumstances, for users of entire audiovisual and other works not currently covered, the law should be clear that any such exemption does not extend to works for which the copyright owner has employed technical measures to limit unauthorized copying.

Finally, unlicensed remote access and public performance of popular audiovisual entertainment like movies, videos and TV shows should not be allowed under Section 108. It is obvious that remote access and public performance of this type of material would directly compete with the normal exploitation of these works.

Sincerely,

Attachment

DIGITAL WATERMARK TECHNOLOGIES
Applications in P2P Networks

P2P Digital Watermark Working Group

DIGITAL WATERMARKING
ALLIANCE

TABLE OF CONTENTS

TABLE OF CONTENTS.....

INTRODUCTION 3

PDWG MISSION .....

DIGITAL WATERMARKING OVERVIEW 4
- O BACKGROUND 4
- O WORKFLOW.....5

USAGE CASES 6
- O USAGE CASE 1 – RESPOND BY SUBSTITUTING ONE WATERMARKED FILE FOR A DIFFERENT VERSION OF THE FILE OR RELATED INFORMATION 6
- O USAGE CASE 2 – RESPOND BY ENABLING A TRANSACTION, AUTHORIZING THE USE OF, OR OTHERWISE MONETIZING THE PARTICULAR USE OF A WATERMARKED FILE (THROUGH ADVERTISING, SUBSCRIPTION, PAID DOWNLOAD, OR OTHER MEANS).....6
- O USAGE CASE 3 - ENHANCE CONSUMER EXPERIENCE BY ENABLING ACCESS TO RELATED MATERIALS.....7
- O USAGE CASE 4 – RESPOND BY ALLOWING OR BLOCKING RETRANSMISSION OF A FILE WITH A PARTICULARWATERMARK 7
- O USAGE CASE 5 – ENHANCE P2P INFRASTRUCTURE BY REPORTING MEASUREMENTS TO MEASUREMENT SERVICES.....8

CONCLUSION .....

CONTACT INFORMATION 9

APPENDIX 10

INTRODUCTION

This informational paper is intended to provide a high-level overview of how digital watermarks can be used in peer-to-peer (P2P) networks to enable new legitimate channels for content distribution, provide infrastructure capabilities that enable enhanced consumer experiences, and support content management activities. For this potential to be realized, all constituents in the content creation, distribution, and usage chain must be willing to agree to and implement certain obligations. Content packaging specifications would have to be defined in a collaborative process. Digital watermark technology vendors would have to upgrade their technologies to carry and detect this specified packaged content if they are not already capable of doing so. Content rightsholders would need to mark content with standardized payloads (i.e., the data carried by the digital watermark). P2P clients would have to securely include the mechanisms to detect and respond to standardized payloads. The bulk of this paper is a description of how the embedding of, detection of, and response to digital watermarks can work to enable monitoring (e.g., usage ratings), triggers (e.g., usage authorizations, enhanced consumer experiences), and other content management activities.

PDWG MISSION

The mission of the P2P Digital Watermark Working Group (PDWG) is to work jointly and cooperatively with leading content and technology companies to describe appropriate and voluntary best practices for the use of digital watermarking to 1) establish such practices for the deployment of watermarking technology implementations as a step to facilitate the legitimate consumption of licensed content through the P2P distribution channel; 2) provide P2P systems with the ability to effectively identify infringing copyrighted content; and 3) ensure that the watermark methods and solutions favored by content rightsholders and watermark technology providers can be scaled effectively by P2P network operators.

ABOUT THE AUTHORS

Participants include DCIA Member organizations and the DCIA; digital watermarking technology and solution providers and the Digital Watermarking Alliance (DWA); and copyright owners, including representatives from motion picture studios and the Motion Picture Association of America (MPAA).

DIGITAL WATERMARKING OVERVIEW

BACKGROUND

Digital watermarks are digital data elements that are embedded into actual content—not carried in the header—so the elements survive analog conversion and standard processing, such as conversion to MP3s or changes in file/media formats. Digital watermarks may be embedded into, and read from, video, audio and still images to enhance the user experience, facilitate business rules, and enrich the media ecosystem as a whole by allowing all content to be self-identifying or carry information that may trigger a defined behavior. Digital watermarking differs from pattern matching (fingerprinting) in that it is not based on statistical matches against databases of known content. Rather, digital watermarks are the equivalent of placing information within the content itself, enabling detection in stand-alone or connected applications throughout the distribution channel and at play-out. In its most common form, the digital watermark data is not perceptible to the human ear or eye, but can be read by computers. One metric for determining whether a digital watermark is acceptably robust is that, when it is embedded at an imperceptible level, it cannot be stripped out without noticeably degrading the host content.

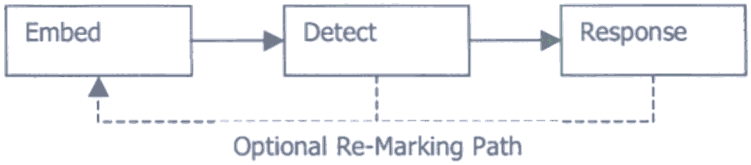
The digital data carried by a watermark can consist of any information deemed relevant for a specific application or usage model, but typically falls into two categories: 1) triggers that indicate some action should be taken (e.g., copy control information (CCI), 'flags' or trigger bits); and 2) identifiers that provide information, usually about the content, the distribution service, and/or the player/client (e.g., media serial numbers, service identifier, player or client identifier). Standards for both the structure and the semantics for conveying both categories of information must be agreed upon for a useful P2P watermark detection ecosystem and business regime to develop. Some of this work has already been tackled by other bodies and could be used as a starting point here (e.g., CCI within ATSC and CEA, Media IDs within ISAN).

Digital watermarks are in extensive use around the world, with billions of digitally watermarked objects and hundreds of millions of detectors in use for broadcast monitoring, copy protection, copyright notification, and forensic tracking applications. Major record labels and movie studios currently use digital watermarks to track content in production and prior to release to the public. This effort has led to a significant reduction in illegitimate use of pre-release music and movies, and has resulted in arrests by the FBI of individuals trafficking in screener copies of movies.

In addition, a number of digital watermarking providers are helping major content rightsholders in the media and entertainment industry today to mark currently distributed movies and music with media serial numbers. As will be discussed later, this effort is establishing an ecosystem of content that could be leveraged to facilitate the creation of legitimate, new P2P content distribution offerings. Other examples of the use of digital watermarks can be found in the Appendix.

WORKFLOW

At the highest level, the digital watermarking workflow consists of three activities that all build on each other and the contextual information provided at each stage to enable increasingly rich and interactive applications.



Embed: At one or more locations in the distribution channel, a digital watermark may be embedded to trigger an action or identify the content, distribution service, and/or player/client at varying levels of granularity. Identifiers can range from, for example, the general title of a work and/or service provider name to the specific, uniquely identifiable copy, service endpoint, or player/client. The mark can be embedded in the source during content creation and preparation, at any point in the distribution chain, and/or in the player/client following some activity, such as completion of an authorizing transaction or further reproduction or distribution of the content.

Detect: The counterpoint to Embed is the Detect step, which forms the foundation for subsequent actions. The watermark may be detected at one or more locations in the content creation and distribution workflow including in conjunction with other operations (caching, routing, etc.).

Response: Once detected, a wide variety of responses are enabled based on the data carried in the watermark, or referenced in response to the presence of the watermark. These are the identification and trigger responses discussed earlier.

Note that the P2P client (application) can incorporate other applications or plug-ins in addition to watermark detection and response application, such as data hash evaluators, acoustic fingerprint analyzers, and metadata readers. When used in conjunction with watermark detection and response, they empower a more robust detection and response environment.

The following Usage Cases are examples of the benefits that watermark embedding, detection, and response can deliver to the artist/rightsholder, distributor, service provider, end-user, and media ecosystem as a whole.

USAGE CASES

1. Respond by substituting one watermarked file for a different version of the file or related information
2. Respond by enabling a transaction, authorizing the use of, or otherwise monetizing the particular use of a watermarked file (through advertising, subscription, paid download, or other means)
3. Enhance consumer experience by enabling access to related materials
4. Respond by allowing or blocking retransmission of a file with a particular watermark
5. Enhance P2P infrastructure by reporting measurements to measurement services

USAGE CASE 1 – RESPOND BY SUBSTITUTING ONE WATERMARKED FILE FOR A DIFFERENT VERSION OF THE FILE OR RELATED INFORMATION

The P2P system (all elements making up a P2P network, including the peers, trackers, and other components) recognizes that the content being searched for as represented by a given file is permitted to be redistributed via this particular P2P application to or from this specific user, but that this particular file is not authorized, and therefore substitutes an authorized version of this content file to be downloaded, opened, or uploaded for redistribution by the user, as the case may be. An example of this implementation is a situation in which the watermark identifies the file, the system checks with a registry or determines via some other analysis that the particular instance of the content in the P2P system is problematic (e.g., the elements have somehow become corrupted), and the system redirects the download to another instance of the content.

USAGE CASE 2 – RESPOND BY ENABLING A TRANSACTION, AUTHORIZING THE USE OF, OR OTHERWISE MONETIZING THE PARTICULAR USE OF A WATERMARKED FILE (THROUGH ADVERTISING, SUBSCRIPTION, PAID DOWNLOAD, OR OTHER MEANS)

The P2P system recognizes through detection of the digital watermark that the content being searched for as represented by a given file is permitted to be redistributed via this particular P2P application to or from this specific user following a transaction in accordance with the agreement between the consumer and artist/rights holder. For example, the user agrees to either not interfere with ads delivered with the content if the content is played back at no charge, or pay a fee to receive and view the content without ads (e.g., paid download or subscription). Two specific examples are:

User downloads a video content file of a copyrighted work that has been watermarked (and may contain other identifiers) indicating that the file is for authorized P2P redistribution pursuant to requiring that a pre-roll ad be viewed and at least one interactive choice must be made by the user related to such commercial message (e.g., choosing the color of a car for an animated test drive).

User downloads a video content file of a copyrighted work that has been watermarked (and may contain other identifiers) indicating that the file is for P2P redistribution pursuant to agreeing to make a payment for viewing, which the user may charge to a credit card or PayPal account. The P2P application would then initiate a transaction to enable the download in accordance with these terms.

USAGE CASE 3 - ENHANCE CONSUMER EXPERIENCE BY ENABLING ACCESS TO RELATED MATERIALS

The P2P system recognizes that the content being searched for as represented by a given file is permitted to access related material and features such as:

1. Interactivity with an online site containing bonus material, games, and other benefits (e.g., online credits, discount coupons);
2. Downloadable bonus content, software, and other benefits;
3. Access to on-screen prompts and interactivity, such as hot spots that provide information about the content; and/or
4. Connection to a related online community or store.

In this scenario, the content rightsholder creates an enhanced experience that motivates the consumer to seek out the legitimate files being distributed via the legitimate infrastructure.

USAGE CASE 4 – RESPOND BY ALLOWING OR BLOCKING RETRANSMISSION OF A FILE WITH A PARTICULAR WATERMARK

The P2P system recognizes through detection of the digital watermark that a given file is authorized to be redistributed via this particular P2P application to or from this specific user, and therefore allows or prevents the file from being downloaded, opened, or uploaded for redistribution by the user. In the case where the digital watermark is used to signal authorization, the detecting application or element enables the processing of that file in accordance with the terms of the authorization. When the watermark is used to signal that a particular use is not authorized, the detecting application or element would limit further downloading, uploading, or playback accordingly. A P2P application might treat unmarked files differently depending on best practices for the given model. For example, in a security-focused environment, a watermark might serve as an indication of a trusted source, and an application might allow uploading of only those files that are securely marked. This case directly facilitates the development of a legitimate P2P content distribution and e-commerce environment by providing greater certainty for consumers with respect to the source and integrity of the content acquired through legitimate P2P services and by giving the artist/rightsholder comfort that the terms under which they are distributing the content will be respected.

Examples

- When a user attempts to download a video content file of a copyrighted work that has been watermarked (and may contain other identifiers), the P2P system detects and responds appropriately to data that indicates whether or not the file is for use in a P2P environment.
- When a user downloads a video content file of a copyrighted work that has been watermarked (and may contain other identifiers), the P2P system detects and responds appropriately to data that indicates whether or not the file has been authorized for this user to view by either playing/storing or not playing/storing the file.
- Similar to the first example, when a user places in a shared folder a video content file of a copyrighted work that has been watermarked (and may contain other identifiers), the P2P system detects and responds appropriately to data that indicates whether or not the file is authorized for use in a P2P environment, and determines whether to allow uploading or playback of the file.

USAGE CASE 5 – ENHANCE P2P INFRASTRUCTURE BY REPORTING MEASUREMENTS TO MEASUREMENT SERVICES

Once a digital watermark is detected, the P2P system gathers and sends anonymous data about the file and its use to a data aggregation and processing system in accordance with user agreements and appropriate privacy safeguards. The monitoring information can then be used to more accurately determine usage patterns and related information in a more precise manner than the statistical methods used in traditional broadcasting. Potential uses of this anonymous monitoring information include as a resource for determining ad rates and artists'/rightsholders' compensation and/or identifying emerging popular trends in content-type and on-line activity. (See Appendix for additional information).

CONCLUSION

This informational paper has articulated a high-level overview of how digital watermarks can be used in P2P networks to enable new legitimate channels for content distribution, provide infrastructure capabilities that enable enhanced consumer experiences, and support content management activities. The Usage Cases illustrate how consumers, artists/rightsholders, P2P system operators, and other players in this ecosystem can benefit from the adoption of watermark technology. The collection of Usage Cases is by no means complete. Readers of this report are encouraged to submit additional Usage Cases to the DCIA.

For this potential to be realized, all constituents in the content creation, distribution, and usage chain must be willing to agree to and implement certain obligations. Content packaging specifications would have to be defined in a collaborative process. Digital watermark technology vendors would have to upgrade their technologies to carry and detect this specified packaged content if they are not already capable of doing so. Content rightsholders would need to mark content with standardized payloads (i.e., the data carried by the watermark). P2P clients would have to securely include the mechanisms to detect and respond to standardized payloads.

This white paper outlines how digital watermarks can be effectively used in P2P networks to provide benefits to all constituents: users, P2P network operators, content service providers and content rightsholders. There are several technological approaches (such as content fingerprinting) that provide complementary alternatives to watermarks to support the identified Usage Cases. It is the intent of the DCIA to investigate all such categories of technologies and enable P2P infrastructures that support all viable technology approaches that can enhance the P2P ecosystem.

CONTACT INFORMATION

P2P Digital Watermark Working Group Chairman
Les Ottolenghi, Chairman, President & Co-Founder
INTENT MediaWorks
www.intentmediaworks.net
les@intentmediaworks.net

Distributed Computing Industry Association (DCIA)
www.dcia.info
Marty Lafferty, Chief Executive Officer
marty@dcia.info

Digital Watermarking Alliance (DWA)
www.digtitalwatermarkingalliance.org
Reed Stager, Chairman
rstager@digimarc.com

Motion Picture Association of America (MPAA)
www.mpaa.org
Brad Hunt, Chief Technology Officer
PDWG@mpaa.org

APPENDIX

Monitoring makes use of digital watermarks to facilitate higher-level business processes at a business-to-business level. When projecting how embedded marks could be used in the P2P environment for monitoring and measurement purposes, it is useful to discuss how they are used today in other situations.

Broadcast monitoring enables content rightsholders and distributors to track the dissemination of content. Broadcast content can be embedded with a unique, persistent identifier (e.g., a payload indicating distributor, date and time information). Detectors are placed in major markets, where the broadcasts are received and processed. The digital watermark is decoded and used to reference complementary metadata in a database, resulting in reports sent to the appropriate parties. Broadcast verification reports can include the specific media outlet, the market, the detection time, the program within which the content aired, and whether it played in its entirety (for audio and video). Millions of broadcast advertisements, promotions, programs, sporting events, news events, etc. currently carry some form of digital watermark.

An example of broadcast monitoring involves using digital watermarks embedded in news stories, ads, and promotions. A detector infrastructure, monitoring radio and TV stations, reports which news stories, ads, and promotions are used, and when, where, and for how long they are aired. The report is accessible to the client within minutes to hours of the broadcast.

The same watermark embedded in broadcast content could be detected online, used to uniquely identify the material, and then enable the Usage Cases discussed in this document.

Similarly, still images can be digitally watermarked and enabled. An example of Internet monitoring of still images involves embedding a content ID in a digital photograph presented on the owner's website. When inappropriate use of the photograph is detected a report can be sent to the content owner. This can lead to the photograph being removed, or, more beneficially, properly licensed. Both of these actions potentially provide more choices to consumers, and increase revenues for distribution services, technology providers and rightsholders.