**Informative Session on Limitations and Exceptions**

**Geneva November 3rd 2008**

**Presentation of the study entitled**

**"Automated Rights Management Systems and Copyright limitations and Exceptions"**

**By**

**Nic Garnett**

**Principal Consultant, Interight**

## I. The Issues

### A. The Central Issue Addressed in the Study

The central issue which the Study attempts to address can be stated in a few simple propositions:

- Most rights holders consider the use of Technical Protection Measures (TPMs), Rights Management Information (RMI) systems and other automated rights managements tools (collectively "ARM technologies") is essential for the implementation of copyright protection in the digital environment;

- Copyright law embodies limits to the scope of the protection it grants to rights holders. These limits are expressed through limitations and exceptions (collectively "exceptions"), through limits on terms of protection and through the use of compulsory licensing schemes;

- Many implementations of ARM technologies have the effect of extending (or have the potential to extend) the scope of content protection beyond the limits set by the copyright law;

- Generally, ARM technologies are unable, qua technologies, to recognize and enforce these limits, particularly when the limits are established contextually;

- Given the ease of reproduction and distribution of content in the digital environment, distribution channels utilizing ARM technologies cannot in practical terms co-exist with unprotected distribution channels

## B. Subset of Issues

There are a number of other issues which have to be taken into account in addressing the central issue:

- The digital environment is highly complex network and becoming more so as the Worldwide Web becomes more participative;

- The technology revolution which is driving the Information Society is changing profoundly both the nature of the activities encompassed within copyright laws and the ways in which such activities are performed. An example of this is in the field of education where life time learning for all has become a common objective in many systems and heavy use is made of technology in pursuit of the objective.

- Copyright laws all contain a complex matrix of rights and privileges in which the application of exceptions is in many cases a cumulative process. Consider the case of a student with a visual disability accessing works for the purposes of private research. Under some copyright laws, both an accessibility and a private use exception would apply. Accordingly, a proper evaluation of the function of certain exceptions in the digital environment as well as the impact of ARM technologies on these exceptions has to take account of the interrelationship between different rights and privileges.

- There are many different kinds of ARM technologies and different proprietary solutions within each area of technology. In the field of Digital Rights Management (DRM) technology for protecting music, leading examples include FairPlay (Apple); Windows Rights Management (Microsoft); Helix (Real Networks). Interoperability is a major issue but developers of different systems can only be expected to standardize their systems where compelled to do so by law or where standardization advances their commercial objectives.

- Where the limits to certain components of copyright protection, starting with the right of reproduction, are expressed through exceptions, those exceptions are subject to the 3 step test laid out initially in Article 9(2) of the Berne Convention. Accordingly, while ARM technologies can be deployed to provide innovative ways to implement exceptions in the digital space, they can also create viable transactional alternatives to the exceptions. In other words, the technical

possibilities may arguably extend the scope of the normal exploitation of a work with a corresponding reduction in the permissible scope of an exception applying the 3 step test.

## II. The Study

### A. Extended Executive Summary

The origin of the study lies in a perceived need to address a major structural issue in the relationship between enforcement of traditional copyright norms and advanced technologies developed and utilized for content protection. The intent was to find, in at least some areas, a reconciliation of the workings of copyright systems and ARM technologies so that, in the digital environment, at least within these areas, the essential balance between the interests of creators and user of copyright works could be maintained.

It should be made clear from the outset that there was never any attempt to discover or devise an all embracing solution or any kind of resolution that required either rightsholders or users in any category to compromise their established rights and privileges.

Another important qualifier is that while the study implicitly recognizes the potential for rightsholders to abuse the power of ARM technologies it proceeds on the basis that the technologies are inherently neutral. By the same token, the inability of these technologies to enforce the limits to content protection mandated by law imputes no intention on the part of rightsholders, through their use, to exceed their legal entitlement.

The study seeks to provide a workable focus within relevant fields of application for examining the potential for synchronizing the functionality of copyright law and ARM technologies. Accordingly, the law and application of ARM technologies were examined in relation to first, access to content by people with visual disabilities and second, distance education. To anchor the study still further in the real world, the copyright laws of five countries were reviewed in detail and field research was conducted in each territory. The latter effort facilitated production of detailed case studies of existing operations illustrating, for the most part, promising applications of ARM technologies in manner consistent with copyright law.

The international copyright norms and national implementations are reviewed in detail in Chapter 1 (Review of relevant International Law); in Chapter 4 (National Law and Practice) and in the detailed legal analysis contained in the Annex. The review and analysis is self-explanatory and requires no further comment here other than to point that in certain jurisdictions the regulatory framework includes detailed provisions as to the implantation of certain exceptions. The extent and complexity of these provisions perhaps explains the move towards voluntary licensing mechanisms and, possibility, of using technologies to automate the licensing processes.

A major theme of the study is to help build cross disciplinary understanding of the relationship between enforcement of copyright norms and the parallel effort of regulating use of content through technology. With this in mind, Chapter 2 attempts to explain the concept of one form of ARM technology known as Digital Rights Management or DRM. In this connection, two considerations are to be noted. First, the cross disciplinary effort in a study of this kind is necessarily something of a compromise and relies on the indulgence of experts on both sides of the divide – lawyers and policy makers on the one hand and computer scientists and engineers on the other.

The second consideration is that, for the general reader, the range of technologies within the general designation of ARM technologies can seem somewhat bewildering. Of these, DRM has received a great deal of attention. It is discussed at length in the study first because of its purported ubiquity in rights management and secondly because of its position as the focus of those concerned with preserving established content access and usage privileges in the digital environment. DRM however should be understood as being but one of several kinds of ARM technologies and one which, at least in the field of digital music services, appears at present to be declining in importance. It is therefore worth pausing in this summary to provide a basic overview of the ARM technologies and their respective functions.

**Technology Solutions: General**

The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty reference ARM technologies in two categories:

- Technical Protection Measures or TPMs;
- Rights Management Information or RMI

(There are important ARM technologies which are not referenced in the treaties)

In general terms, TPMs are systems or applications which block access to and/ or use of digital content on an absolute or conditional basis. RMI systems on the other hand are systems supporting the automated identification of content and certain attributes of that content. RMI systems, by themselves, apply no control on access to or use of the content they identify (but they can support associated systems or applications which do).

TPMs are not defined in either the WCT or the WPPT; RMI is defined as follows:

> *As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public*

While the categorization of the classes of technological solutions used in the WCT and WPPT is accurate, it should be understood that the systems to which they refer are not mutually exclusive. In fact their use can be closely interrelated and thus understanding the relationship between TPMs and RMI is fundamental to understanding how technology-based rights management works and how it is evolving.

**Technology Solutions: Explanations**

**TPMs:**

As stated above, the function of a TPM is to restrict access to or usage of content either absolutely or on a conditional basis. A copy prevention TPM such as CSS is an example of the former; FairPlay, the DRM system used on the iPod, is an example of the latter. TPMs are used at the discretion of the rights holder or a partner in the distribution chain to give effect to the business model and rules chosen for exploiting the content in question.

From a very basic technical perspective TPMs can be broken down into 2 categories: those technologies used to protect the content and those technologies that are used to control access to systems through which the content is delivered.

Category 1: in this area, technology is used to encrypt the content so that it cannot be used without being decrypted. In encrypted form the content can therefore be transmitted throughout the network without risk of its being used without authorization. The key which is required to decrypt the content, allowing it to be used in its normal form, is made available to a user ideally in a way which is unique to that user and where the key can only be used if the user complies with certain conditions for use of the content. Such a condition might include, for example, paying for each use made of a piece of content. These technologies were developed to facilitate secure rights management in open networks such as the Web.

A slightly different application of this technology is in relation to the use of content on particular devices. Thus with the CSS system the audio-visual content on a DVD Video disc is encrypted. The key necessary for its decryption is embedded in the playback device (a DVD player) on which authorized use of the DVD can be made.

Category 2: in this area technology is used to control the access by users (or devices) to closed networks where content is accessible provided it stays within the closed network and is used according to the rules in force within the network. This technology focuses on the systems used for securely authenticating users of the system. An example of this would be a proprietary cable network to which users subscribe by paying a monthly subscription fee.

As always, hybrid systems combining elements of both approaches are also commonly found. Thus, a closed cable network may also employ systems for encrypting the content within that network, thereby enhancing its overall security.

**RMI Systems**

According to the definition within the WIPO Treaties, RMI systems encompass 2 levels:

- Information about the content
- Coding associated with the content as delivered embodying that information.

Examples of the first would include such identifiers as the Digital Object Identifier (DOI), a URL, and an ISO standard identifier such as the ISBN or ISRC codes. As associated directly with the content, these information or identifier systems are used primarily to create links with detailed metadata resources located on remote servers.

Coding systems used for associating the identifier with content (level 2) include embedded metadata tags (e.g. ID3 tags) and digital watermarking.

**Embedded Data Systems**

With embedded metadata systems, the linking mechanism is an identification code or tag contained within, for example, an encoded music file. The ID3 tag is just such an embedded code. It is a metadata container most often used in conjunction with the MP3 audio file format which allows information such as the title, artist, album, track number, or other information about the file to be stored in the file itself.

**Watermarking**

Watermarking works by adding a watermark code – a string of binary numbers - to a piece of content as it is being encoded into a particular electronic file format. This can be done with any form of content: audio; audio-visual; text; images. The watermark is imperceptible to the user: it cannot be heard nor seen and in no way interferes with the enjoyment of the content in question.

Once the content file is equipped with a watermark, the use of that item of content can be easily tracked across networks and different user applications. Monitoring systems are installed within the networks and user applications which monitor the watermarks of different content items transmitted or used. Information about usage instances associated with identified watermarks is then fed back to central databases which match the watermarks to the corresponding metadata stored there for each content item.

Watermarking has another important use. Because it is possible to include other information in the watermark code, the system can also be used to keep a designated user within an authorized field of activity. If the designated user attempts to use the item of content in an unauthorized manner, the watermark can trigger a mechanism effectively blocking the unauthorized use. In the same way, if a piece of content, identified by the watermark as being delivered to a specific user for a particular purpose, comes to be used for a different purpose or by a user other than the one designated by the watermark, a

challenge can be presented to the original user regarding subsequent unauthorized use. This process of forensic tracing as it has come to be known can be very useful to rights holders.

Another key feature of watermarking is that since every item of content is equipped with a specific watermark the process of identifying the content is extremely accurate and efficient.

**Other ARM technology systems**

Another form of ARM technology – one that is becoming increasingly talked about – is that of content fingerprinting. It is dealt with separately here as it does not fall within the definitions of RMI systems as contained within the WIPO Treaties.

Fingerprinting involves the analysis of a specific content file and the extraction from that file of a set of measurements, related to particular characteristics of the content, which are unique to that particular content file. This set of measurements is then assigned a particular code which represents its "fingerprint". As with watermarking, this fingerprint code is then linked back to a central database where the code is matched to the metadata corresponding to the particular piece of content.

In the case of fingerprinting, each content item has only to be processed once – to extract the fingerprint. Once this has been done, the content item can be tracked wherever it travels within a network, in whatever format it is encoded and through whatever user application it is accessed and used. The only requirement is that somewhere in the network or in application the end user employs to access and use the content there exists a mechanism for taking the same measurements of the content and computing the appropriate fingerprinting codes for the content.

The advantages of fingerprinting include the ubiquity of the system and its ability to monitor the transmission and use of content throughout a particular network without the need for pre-installing a specific code (as is the case for watermarking). And, as with watermarking, by supporting fingerprint tracking with appropriate technologies it is possible to use that tracking to prevent the use of content beyond the scope of an authorized usage model. An example of this would be in policing the perimeter of an authorized P2P file sharing network: identified content would be prevented from transmitted outside the protected network area.

An early use of audio fingerprinting technology has been in the remote, automated monitoring of radio broadcasting. Instead of having a collective copyright administration agency manually processing broadcasting logs prepared and delivered by a given broadcasting entity, systems based on fingerprinting can perform an identical function with great accuracy at a lower cost.

Again, it is important to note that watermarking and fingerprinting content identification systems are not mutually exclusive. The systems can be used very effectively in tandem to provide maximum security and information retrieval capability.

The preceding paragraphs hopefully provide a basic guide to the complex and still evolving landscape of ARM technologies to augment explanations contained within the study. Another approach to better understanding the field of ARM technologies and their application is also used in the study, that of differentiating conceptually between the notions of content management and rights management. This is introduced at the beginning of Chapter 2 and seeks to explain how the rights in content can be managed independently of the technologies making them available to (although not necessarily accessible to or usable by) end users (consumers). This separation of functions with regard to content and rights is at the heart of advanced DRM systems.

**Fields of Application**

Chapter 3 of the study surveys the target fields of application, dealing first with the needs of visually impaired people and then with distance education.

On November 3rd 2003 speaking at the Information Meeting which then preceded the WIPO Standing Committee on Copyright and Related Rights David Mann of the World Blind Union made the following statement:

> *If we accept that access to information is a right, then it follows that any impediment to information is a denial of that. Barriers can be economic; they can be technological, and they can be legal.*

The statement embodies the conundrum facing visually impaired people in relation to DRM: on the one hand, technology facilitates their access to and use of content in ways and with ease heretofore unimaginable; on the other, DRM technology serves in many cases to negate much of that capability.

Since the publication of the study the Board of Directors of the Daisy Consortium, the body responsible for the Digital Accessible Information System talking book standard, has issued a clear policy statement on DRM. It states in part:

> *The DAISY Board does not in any way promote DRM. The Board believes that DRM limits the legitimate use of digital publications by persons who are blind and print disabled. Persons who use Assistive Technology commonly manipulate digital publications in ways that most people without disabilities do not understand. Moving an eBook to a portable device with refreshable braille, or copying it to a hand held device for reading "on the go" are two simple examples of common legitimate usage that are prevented by DRM. From a content management or library perspective, DRM can complicate or make impossible the upgrade of digital collections to new and future technologies. For these and other sound reasons, the DAISY Board is publishing this statement to*

> *discourage the use of traditional DRM encryption whenever possible.*

Publishers, understandably, have a view which is governed by their commercial imperatives and their perspective of the market as whole. The study notes that while there is general sympathy on the part of publishers with the position of visually impaired people, there is also growing concern with the ability of technology to threaten their fundamental rights as well as those of the authors they represent. This position was succinctly expressed by Mr. Michael Keplinger, Deputy Director General, WIPO at the IPA Congress in Seoul in May of 2008:

> *One of the most serious challenges the publishing industry faces today is that of copyright infringement, or piracy. Piracy takes on a new dimension in the digital environment, where millions of copies of published works can be copied without authorization and distributed to more than a billion online users, globally, and with the simple click of a mouse. The ease of copying, the difficulty in detection, and the scale of reproduction and dissemination of infringing copies, poses significant problems to the publishing industry and the intellectual property community as a whole.*

There is less focused concern expressed about DRM in the field of distance learning on the side of users of content. The situation faced by the publishers of materials used in distance learning however has however received publicity:

> *College students are increasingly downloading illegal copies of textbooks online, employing the same file-trading technologies used to download music and movies. Feeling threatened, book publishers are stepping up efforts to stop the online piracy.*
>
> *One Web site, called Textbook Torrents, promises more than 5,000 textbooks for download in PDF format, complete with the original textbook layout and full-color illustrations. Users must simply set up a free account and download a free software program that uses a popular peer-to-peer system called BitTorrent. Other textbook-download sites are even easier to use, offering digital books at the click of a mouse.*
>
> *"There are very few scanned textbooks in circulation, and that's what we're here to change," says a welcome message on the Textbook Torrents site. "Chances are you have some textbooks sitting around, so pick up a scanner and start scanning it!"*[1]

[The Textbook Torrents site is no longer active; there are others that are]

---

[1] The Chronicle of Higher Education; Tuesday July 1 2008 available here: http://chronicle.com/free/2008/07/3623n.htm

With hindsight it is probably fair to conclude that in addressing the field of distance education the study was over ambitious. Education in all forms has its own vast ecosystem, an ecosystem in which the role of copyright law generally is probably significantly out of alignment with the technical, operational and commercial realities of the field. Until more work is done to address possible realignment of copyright law in the sector, trying to envisage the role of ARM technologies in the field is speculative at best.

The needs and rights of visually impaired people present an entirely different case, one which is at core an exercise in risk analysis and management. Access to information in the digital environment by visually impaired people is being obstructed by the use of certain kinds of DRM technology. That use is justified by rights holders on the basis of its ability to reduce the threat to their works from piracy. To the extent that both propositions can be objectively assessed they should be. It was not the function of the study to do so. The study instead proposes a more pragmatic way forward: devising systems which while facilitating access provide rights holders with the protection that their works deserve and to which they are entitled under copyright law. The study further proposes that the use of ARM technologies in certain contexts may well provide the basis for a balanced solution, recalling once again the sagacity of the late Charles Clark and his famous utterance: "The answer to the machine is in the machine".

**The interface of law and technology**

This last observation leads logically to the central thesis of the study as developed in chapters 5 and 6 and which can be stated in a few simple propositions:

- ARM technologies, including DRM, are unable, per se, to give meaningful effect to exceptions because:
    - ✓ As noted above, removing protection from content to facilitate use pursuant to an exception to copyright effectively negates the use of protection where no exceptions apply
    - ✓ DRM technology is already highly complex: having it interpret contextual considerations inherent in the application of exceptions represents a quantum leap in complexity.
- ARM technologies in most deployments require ongoing operational management by some central authority
- The central authority which manages an ARM technology deployment can also act as a Trusted Intermediary and should comply with generally accepted standards in the performance of its role

- Some beneficiaries of certain exceptions to copyright law – visually impaired people are one such constituency – often rely, in part, on institutional support to meet some of their needs. In some instances, the institutions are appropriately structured to act as the Trusted Intermediary responsible for deploying an ARM technology to support its community while acting as the trusted interface with commercial rights holders and service providers and their ARM enabled networks and applications.

- Once identified a suitable Trusted Intermediary is able to establish a secure network within which the community of users can have access to content in the manner provided for by copyright law.

The best statement regarding the inability of DRM to address the complexity of exceptions and limitations is that of Professor Ed Felton. He deals first with the inability of DRM to implement fair use as it exists in US copyright law:

> *The legal definition of fair use is, by computer scientists' standards, maddeningly vague. No enumeration of fair uses is provided. There is not even a precise algorithm for deciding whether a particular use is fair. Instead, the law says that judges should make case-by-case decisions based on four factors: the nature of the use; the nature of the original work; the portion of the original work used; and the effect of the use on the market. The law does not say exactly how these factors should be evaluated or even how the factors should be weighted against one another.*
>
> *To a computer scientist, such imprecision is a bug*

The importance of this statement resides not only in its highlighting of the problem with uncodified exception cases; it also underlines the very different approach of lawyers and engineers to the process of policy definition and implementation.

Professor Felton's analysis however goes beyond the obvious difficulty of implementing the case specific fair use exception:

> *If DRM systems can't make the right judgment in every case, perhaps they can get some special cases right. Perhaps they can allow backup copies or personal use within the home. Perhaps these special cases are simple enough that they can be reasonably approximated.*
>
> *But even these seemingly simple cases are more difficult than they might initially seem. A backup, for instance, is most useful if it can be restored on a different machine (in case the original machine*

> *breaks). But backup cannot simply provide a mechanism for moving a file from one machine to another; such a general file transfer facility is a ready loophole for infringers. The solution may involve centralized record keeping, ensuring a backup is not restored too frequently or in too many places, though such record keeping raises privacy issues.*
>
> *The point is not that handling backup is impossible but that it is surprisingly challenging. To date there has been no satisfactory solution to these problems, though it may be because most of the development effort has been (mis)directed toward the effort to build all-encompassing DRM systems. There may be hope, however, for a bottom-up approach that tries to handle a few cases well.*

Professor Felton's reference to "centralized record keeping" is also important, implying as it does the use of some central authority in the administration of some ARM technology based exception implementation model.

**Mediated implementation of exceptions with ARM technology**

The idea of implementing certain exceptions through the use of ARM technologies and Trusted Intermediaries is not new. Indeed it is already commonly used. In order to provide their communities with accessible materials while securing rights holders from risk, organizations such as Bookshare in the USA, Braillenet in France and the National Library for the Blind in Denmark all used implementation of ARM technologies. There are many other working models. Furthermore, this kind of organization of controlled content access through Trusted Intermediaries has much in common with the DRM systems being increasingly used in the workplace to maintain the security of information and work flows.

These intermediaries would in turn utilize some form of ARM technology to ensure that terms upon which it was making the content available were restricted to users with the community it was serving. Equally it would be required to ensure that content made available via its network within that community would remain within that network.

The study concludes by examining this idea in more detail, envisaging a broader application in other fields where exceptions might be implemented on a secure, community basis. It suggests that for the broader development of such models it will be important to establish criteria for identifying suitable intermediaries. It looks at established and emerging models in the sector, identifying certain standards that should be met by entities undertaking the responsibilities of a trusted intermediary.

## B. Updates and Further Thoughts

The bulk of the research for the study was conducted in 2004 and early 2005 and much has happened in the world of ARM technologies since then. The most apparent development has been the current trend away from the use of DRM technology in certain fields coupled with growing interest in other ARM technologies such as fingerprinting. This is particularly the case in the market for digital audio content.

In September 2007 the major US online retailer Amazon launched its DRM-free music download service, offering digital music files in an unencrypted MP3 format. Customers of the service are able to access the content they purchase, store it, move it into other media and even share with friends unconstrained by any technical control. Following this development, the leading online retailer of music, iTunes, followed suit and started offering some DRM-music files on its site. Both companies were following a model initiated earlier by a service called eMusic.

This move towards the delivery of DRM-free audio files was adopted by a number of leading book publishers as well, as reported in the New York Times in March 2008:

> *Some of the largest book publishers in the world are stripping away the anticopying software on digital downloads of audio books. The trend will allow consumers who download audio books to freely transfer these digital files between devices like their computers, iPods and cellphones — and conceivably share them with others. Dropping copying restrictions could also allow a variety of online retailers to start to sell audio book downloads. The publishers hope this openness could spark renewed growth in the audio book business, which generated $923 million in sales last year, according to the Audio Publishers Association.*
>
> *Random House was the first to announce it was backing away from D.R.M., or digital rights management software, the protective wrapping placed around digital files to make them difficult to copy. In a letter sent to its industry partners last month, Random House, the world's largest publisher, announced it would offer all of its audio books as unprotected MP3 files beginning this month, unless retail partners or authors specified otherwise.*
>
> *Penguin Group, the second-largest publisher in the United States behind Random House, now appears set to follow suit. Dick Heffernan, publisher of Penguin Audio, said the company would make all of its audio book titles available for download in the MP3 format on eMusic, the Web's second-largest digital music service after iTunes.*

At the same time focus has shifted to ARM technology solutions involving the use of fingerprinting. In the new model, content providers are seeking ways to require ISPs to equip their networks with applications that monitor content traffic through the use of fingerprinting technology. Content items that are indentified as not being authorized for use within a particular network can then be removed from the network through blocking mechanisms. The theory behind the development is that removing unauthorized content from networks will leave then free for the legitimate and, presumably, paid for content services developed or supported by rights holders. The idea places a heavy responsibility on the fingerprinting technology developers to come up with workable and reliable systems.

Is it possible to conclude that DRM as a form of ARM technology is set to disappear? The answer is a resounding "no" for several reasons.

First, the move away from DRM by the music industry has probably more to do with the way it sees it business best conducted than because of any fundamental challenge to DRM. Other information and entertainment industries, notably the electronic games, television and film industries, are pressing ahead with implementations of DRM and development of business models founded on the controls DRM facilitates. It is perfectly reasonable to anticipate a return to the use of DRM based models by the music industry perhaps as general purpose DRM systems are deployed by other industries.

Second, it is not clear that the alternative ARM technologies and the business models that music industry is currently contemplating will actually be capable of delivering the anticipated returns.

Third, work on many ARM technologies and DRM in particular is progressing rapidly, addressing many of the issues encountered with first generation solutions. Interoperability, while still a problem in many implementations of DRM, is being addressed by initiatives such as that of the Coral consortium. Furthermore, DRM is becoming an increasingly essential part of the network infrastructure in the workplace.

In short, the issues addresses in the study remain alive. Equally, the general limitations of DRM to accommodate exceptions and limitation to copyright, as clearly explained by Professor Felton, remain unresolved. It is fair to conclude therefore that notwithstanding the passage of time the analysis contained within the study and the ideas proposed for resolving, on a workable basis, some of the conflicts between the application of legal norms and technical systems remain entirely valid.