Digital Rights Management

On 13 October 2004, the Network Insight Institute held a seminar entitled 'Digital Rights: Management & Co-operation' centred on issues concerning the distribution and cataloguing of digital goods and co-operation in their management. Katherine Sainty and Clare Cunliffe consider some of the issues discussed in the seminar.

INTRODUCTION

The major Hollywood studios, through the Motion Picture Association of America, have told us to expect a slew of prosecutions for 'copyright theft' of motion pictures and video programs.

This follows similar prosecutions by the recording industry, notably the Napster case. These actions illustrate one important aspect of digital rights management – the protection of digital goods and content.

Another aspect is the digital management of rights and payments. Technological innovation and the ubiquity of the internet have created an opportunity for the centralised distribution of digital content. But the availability of centralised distribution means rights holders need to rethink business models.

Digital content offers advantages for consumers and rights holders alike. It is easy to duplicate (with no loss of quality), compress and distribute. But these advantages increase the ease with which digital content may be redistributed and the incentive to redistribute without the authorisation of rights owners. So business models for the delivery of digital content must strike a balance between robust content protection and the need to 'keep the customer satisfied' by offering well priced, easily accessible and desirable digital content. The interdisciplinary field of digital rights management (**DRM**) can be used to strike a balance between these different, and sometimes competing, priorities.

In this article, we define DRM, identify the key stakeholders involved, and look at some of the key issues to be resolved going forward.

WHAT IS DRM?

DRM is the use of technology to manage copyright and related rights to digital goods and content. The management process continues throughout the lifecycle of the goods and content. The two main components of DRM systems are rights management and copy protection. DRM systems enforce usage rules which are set by users and manage the consequence of usage, for example, payments to rights owners. This is discussed in more detail below.

WHO ARE THE STAKEHOLDERS?

The major stakeholders in relation to the distribution of digital content are content owners, technology companies, carriers and Internet Service Providers (ISPs) and consumers. The interests of these groups are not always aligned. A summary of stakeholder perspectives' follows.

- *Content Owners*

  Content owners, such as record companies, motion picture studios, publishing houses and individual artists, endorse a growth in digital business in addition to (not in substitution for) existing revenue models. Content owners seek reasonable compensation in exchange for use of their intellectual property.

  Content owners are concerned that what is encrypted, can be decrypted. They therefore require robust copy protection mechanisms which can be continually upgraded and renewed to minimise circumvention. Content holders are also concerned with educating consumers about authorised and unauthorised use of digital content. This is one of the key messages that the record companies and studios are seeking to send with their prosecutions.

- *Technology Companies*

  Technology companies, such as makers of home entertainment systems, drive sales of electronic goods in an atmosphere in which digital technology is rapidly developed and embraced. The demand for these goods (e.g. plasma screen and home theatres) is partly driven by the demand for digital content. However, there is also consumer demand for devices which can be used to circumvent copy technology, such as CD and DVD burners. For this reason, there is an inherent tension between content owners and technology companies.

  In some cases, content owners also provide the technology by which digital content is accessed – for example, computer games and pay television work on 'closed' systems, using proprietary technology to provide digital content. This trend is discussed below in the section on 'Technological enforcement of usage restrictions'.

- *Carriers and ISPs*

  It is in the interests of carriers and ISPs to encourage the growth of broadband and wireless based businesses, which depends in part on the availability of digital content. Carriers and ISPs benefit from the sale of telecommunications capacity to consumers and content owners.

- *Consumers*

  Consumers are eager to access digital content, but are resistant to any erosion of their personal rights (real or perceived) through DRM. Consumers may misapprehend the extent of their rights to access and use digital content, especially given the ease of accessing and copying digital content. Some consumers perceive DRM processes, especially in relation to payment and downloading, as complex and restrictive and may also perceive DRM as a threat to their privacy.

Consumers are concerned to ensure DRM is easy to use, interoperable with their existing technology, reasonably priced and compliant with privacy law.

ISSUES GOING FORWARD

DRM involves three major elements:

- the identification and description of digital content and intellectual property rights;
- the technological enforcement of usage restrictions; and
- the legal enforcement by rights holders of their rights.

Identification and description of digital content

To effectively manage and enforce digital content, it is necessary to uniquely identify the content which is being distributed.

There are a number of standard identifiers for content, including the International Standards Organisation identifiers (particularly, the International Standard Audiovisual Number, or ISAN, applicable to audio-visual works), and other identification systems like the Digital Object Identifier.

The issues of whether the identifiers should be subject to standardisation, and whether standardisation should be led by industry or by government are subject to much debate.

As well as being identified, digital content must be described (usually by reference to the author, rights owner, date of publication and originating territory). This description is usually contained in the metadata of the digital content.

Technological enforcement of usage restrictions

Rights holders can set rules to allow or prevent various uses of digital content, which are enforced by copy protection technologies. Copy protection technologies may draw on techniques developed for use in e-commerce and conditional access systems, such as scrambling systems, encrypted cipher keys, and watermark techniques. Sophisticated DRM systems may allow users:

- to download and play, but not copy or forward, digital content;
- to download digital content and integrate it into a user's home network;
- to download digital content for a set period and either 'refresh' rights upon expiry, or have digital content automatically deleted;
- to forward digital content but to prevent forwarding on by recipients; and
- to 'preview' digital content with certain time and usage restrictions.

DRM requires the encryption of digital content and of the accompanying user restrictions. The security levels provided by copy protection technologies will vary according to the value of the content to the rights owner. For example, premium movie content tends to be subject to more sophisticated copy protection technology than other forms of digital content.

Of course, the effectiveness of copy protection technologies will be affected by the form of technology which receives the digital content. For example, a home PC will generally be less secure, and is more easily able to be used to circumvent copy protection technology, than a device like a DVD player (without a DVD burner) or pay television set top box. For this reason, a rights owner's control over digital content tends to be strengthened by the ability to control the equipment used by the consumer. However, this increased control needs to be balanced against the demands of consumers for a convenient technology which does not require a considerable investment in infrastructure.

There is also considerable debate as to whether technological standards should apply to DRM systems. Such standards could be global or regional, government-mandated or industry determined. Agreement on standards would increase interoperability (an important concern from the consumer's perspective) and might lead to more rapid deployment of DRM systems. However, there is a strong resistance to a government sponsored monopoly in DRM technologies. Many stakeholders feel that DRM technology should be given room to develop and the market should be given an opportunity to decide on the best technology.

Legal enforcement of usage restrictions

Rights owners of digital content need to be able to enforce their copy and use restrictions, both via contractual licensing arrangements with users and by enforcing rights under the Digital Agenda provisions.

Content service providers can specify the scope of any licence to use the rights associated with digital content (which may be more or less restrictive than the rights granted under the Digital Agenda provisions of the *Copyright Act 1968* (Cth) (**the Act**), but these contractual terms will only be enforceable against the initial user. The Act provides enforcement measures against unauthorised third parties or unauthorised use by the initial user.

The Act sets out civil and criminal remedies for copyright owners against persons who deal commercially in circumvention devices, or provide services used to circumvent technological protection measures. There are also civil remedies against persons who remove or alter rights management information, or deal in copies of copyright material that has been doctored to remove this information. The Act also provides that carriers and ISPs will not be liable for authorising infringements that occur on their networks (including on websites hosted on their servers but operated independently), by reason only of the fact that the infringement occurred on the facilities provided by the carrier or ISP.

The relevant provisions of the Act will be amended by the *US Free Trade Agreement Implementation Act 2004* (the **USFTA Act**) which was assented to on 16 August 2004 and will come into effect on either 1 January 2005 or the date the Australia-US Free Trade Agreement comes into force, whichever is the later date. It should be noted that the USFTA Act does not implement all of Australia's obligations under the Australia-US Free Trade Agreement. However, the USFTA Act makes some significant changes to the

law applicable to DRM. These are outlined below:

- *Expansion of protection of encoded broadcasts*

  The USFTA Act expands the range of criminal and civil penalties for the unauthorised manufacture, distribution and use of broadcast decoding devices relating to cable or wireless subscription television signal piracy. These actions will now be available to content owners and channel providers, in addition to broadcasters.

- *Carriage service provider liability*

  The USFTA Act provides that the liability of ISPs and carriers for infringement by subscribers will be limited if they satisfy certain conditions. Under the new provisions, a court must determine that infringement has occurred before an ISP will be required to 'take down' material from its servers.

- *Definition of 'material form'*

  This USFTA Act expands the concept of 'material form' to apply to all forms of storage of a work or other subject matter, whether or not they allow further reproductions.

- *Electronic rights management information (**ERMI**)*

  The USFTA Act expands both the definition of ERMI and the scope of actions that may be taken by rights holders against the removal of ERMI.

Of course, the effectiveness of the legislation to some extent depends on consumer awareness. Rights holders are engaged in ongoing campaigns to educate consumers about their rights and obligations under the Act.

CONCLUSION

As DRM continues to evolve, we can expect to see stakeholders seeking solutions which balance their needs and drive DRM development. The call to standardise the applicable technology, the development of accessible, affordable and user friendly DRM technology, the need to educate consumers as to their rights and obligations, the impact of the recent changes to the relevant law and the continuing proliferation and use by consumers of unauthorised content, can all be expected to play a part in this development of DRM.

Katherine Sainty was one of the speakers at the Network Insight Institute seminar and is a partner at Allens Arthur Robinson in Sydney. Clare Cunliffe is a Senior Associate in the same office of Allens Arthur Robinson. More information on the Network Insight Institute seminar on "Digital Rights: Management & Co-operation" is available from the Network Insight Institute's website at http://www.networkinsight.org.

"I'll Have Two Playmates and an Emoticon Please"

Nick Abrahams, Glenda Stubbs and Alan Arnott provide an overview of mobile content regulation in Australia.

INTRODUCTION

The mobile telephone has been transformed from a brick-sized cellular telephone to a slimline sophisticated multi-purpose device weighing less than 75 grams. Today's mobile phone is armed with polyphonic ring tones (polyphonic and now "true tones"), radios, mp3 players, cameras, flashlights and blue tooth headsets, capable of instantaneous wireless transmission of text, audio, images, video and most recently the Multimedia Messaging Service **(MMS).**

Alongside this progression in technology has been a significant increase in the quality of transmissions, most apparent with the advent of 3G technology. 3G technology is faster than prior mobile technologies like GPRS (2.5G), and offers enhanced multimedia capabilities like videoconferencing, streaming video and broadband-type speeds.

Commercially, mobile technologies are presenting a plethora of avenues for financial exploitation. Known as m-commerce, mobile phone users can use their mobile to acquire a range of goods and services. A good example is Telstra and Coca Cola's "Dial-a-Coke" vending machine. This allows Telstra mobile customers to purchase soft drinks via mobile phones. The cost of the drink plus the cost of the call is debited to the user's mobile phone account.

Other areas where providers have been experiencing stellar growth in revenues include SMS/MMS voting/ promotions and content such as ringtones, wallpapers, games and emoticons (the ":)" that people put in emails – yes it has a name).

Like the internet, mobile technologies are also facilitating the wireless transmission of raunchy content. For example, 3G-enabled carrier, Hutchison, is offering "the captivating beauty of every Playmate of the Year since 1960, every Cybergirl of the Month since 2001 and Videogalleries featuring Playboy videoclips ..."[1]. This novel area of mobile adult content definitely presents new challenges for regulators.

Adult content available through mobile phones is currently accessible via the premium rate SMS/MMS 19x services and proprietary network range that is independent of the internet. The range of types of services available include SMS sex, downloadable sexually explicit mobile phone wallpaper, and the "Naked News", a Canadian strip-news program available on m-Vision, Australian media and communications company GoConnect's mobile video distribution platform.

While m-commerce means added convenience for purchasing goods and services, the availability of premium services clearly poses risks to some mobile phone users. Two major concerns have been identified by the Australian Communications Authority