DRM

— "digital rights" or "digital restrictions" management?

Richard Leeming
Red Bee Media

If correctly applied, DRM can be likened to a motorway, providing a seamless high-speed route to content, enabling people to get the content they want, where they want it, quickly and easily. However, if badly applied, heavy handed and overly restrictive, DRM is more like a traffic jam – denying people access to the content they want and crucially denying rights-holders the revenue they want.

This article looks at some of the proprietary DRM systems currently available and argues that we need to start thinking hard about when and how we apply DRM to our precious content.

In 2006, music lovers worldwide have been celebrating the 250th anniversary of Mozart's birth. Although he only lived for 35 years, Mozart composed more than 600 pieces of classical music – most of which are still hugely popular today.

But it's perhaps something of a surprise to discover that one of the key moments of Mozart's early career would today count as *piracy* and be prevented by digital-rights technology.

As a 14-year-old, Mozart travelled to the Vatican and heard Gregorio Allegri's *Miserere*. This piece of music had long been closely guarded by the Vatican and it was forbidden to transcribe it: if you did, you would be excommunicated. Whether Mozart knew this is unknown but, having heard it once, he transcribed it from memory and it became published in London, thus breaking the Vatican's ban.

This is perhaps one of the earliest-known examples of content rights management being overturned. The Vatican may not have been too happy, but music lovers worldwide have benefited for more than two centuries now.

There's little doubt that issues around *digital rights management* (DRM) present one of the key areas of debate in the emerging digital content market.

On the one hand you have rights creators; the record companies, Hollywood studios, TV production companies, broadcasters, and sports organizations who seek to get a financial return on their artistic creations. Then, on the other hand, you have the technology companies, be they distribution platforms or device manufacturers, who want to get the best content onto their platform and recognize the need to meet the requirements of content owners.

And then there are the consumers, the people who actually watch and listen to this stuff, some of whom are paying for it, some of whom are getting it for free in ways they probably shouldn't and most of whom are slightly baffled by the term digital rights management.

All of these parties have differing and conflicting interests, and it's proving hard to reconcile their different needs.

Even the term DRM itself is open to debate. While the simple definition that it is *"any one of several technologies used by publishers or copyright holders to control access to or usage of digital data such as movies, music files or video clips"* is relatively uncontroversial, a growing campaign against DRM suggest the term would better be defined as *Digital Restrictions Management*.

Aside from the philosophical debate, there are:

- commercial concerns that DRM can be anti-competitive or off-putting to consumers;
- legal concerns that DRM over-rides long-standing legal precedents and consumer rights, and
- artistic concerns that DRM stifles creativity.

One thing that does seem certain is that the market for DRM software is booming. According to market research company Jupiter Research, the market will grow to $274 million by 2008 from $36 million in 2003.

The driving forces behind DRM have been around for as long as it has been possible to copy content. British music fans who bought records in the 1980s will be familiar with the phrase "Home taping is killing music". Around that time, the introduction of videotapes led to the 1984 US lawsuit *Sony Corp. vs. Universal City Studios* which eventually led to the US Supreme Court setting an important legal precedent – that a technology cannot be illegal, but the use of it can.

Clearly the advent of digital media makes the demand for DRM even greater as multiple copying of digital content not only becomes easier, quicker and cheaper, but also avoids the quality degradation that happened with analogue content.

DRM technologies

There are many different DRM technologies, so providing an accurate technical description of them is outside the scope of this article.

However, to focus on the needs of the broadcast industry, an early distinction needs to be made between *Conditional Access* and DRM.

Conditional access

Conditional Access (CA) is the system that has traditionally been used to protect TV channels. The standards are tightly-defined and provide a method by which a digital television stream can be scrambled. The only people who can descramble, and thus watch, the picture are those with the right receiving box and valid keys. Clearly these are the people who have paid to receive the service.

A good example of this in action in the UK is on Sky Sports on a Sunday afternoon. Watch the match at home, then go to the nearest pub that is showing the same game and you'll see a simple difference. In the pub, the screen will have an icon depicting a half-empty pint glass in the bottom right hand corner of the picture. This denotes to any visiting spies from Sky Sports that the pub has paid for the premium rights to show the game to paying customers.

Conditional Access works by a combination of *scrambling* and *encryption*.

Alongside the scrambled signal, secret keys are also transmitted. These keys enable the descrambler to work at the receiving end but, to ensure that they are not compromised, they are also encrypted. As well as being scrambled, the keys are regularly changed.

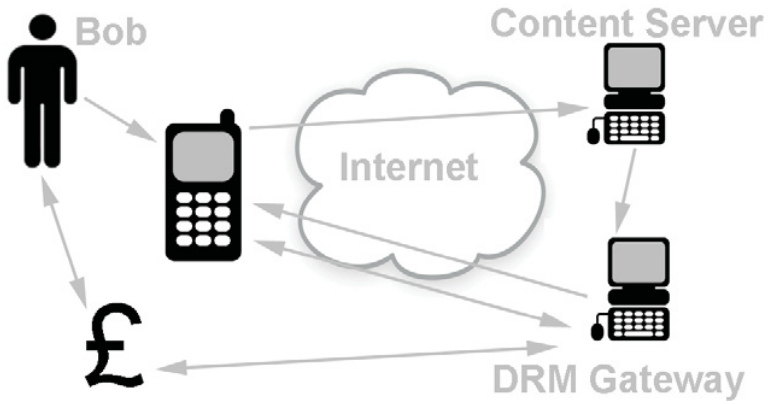
DRM

The main difference between CA and DRM is that DRM is usually applied to a specific piece of content.

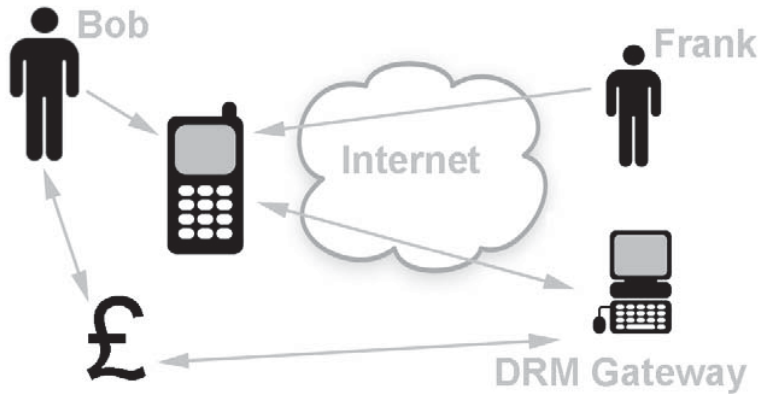
The list of actions covered by DRM are growing even longer, but typically they cover such things as:

- when the content is available;
- how many devices it can be viewed on, or indeed if it can be passed between devices at all;
- how many times it can be viewed;
- how long it is available for ... and so on.

A simple explanation of how DRM systems works is this. It depends on content being secured by an encryption key which is split into two halves, one of which is *private* and one which is *public*.



When a person (e.g. Bob) opts to buy a piece of content – say a music track or a video clip – from an online store, it first passes over the public half of the content encryption key. This is then attached to the digital file by the DRM gateway. The digital file and the public key is then sent to Bob where it is unlocked by his private key ... and the usage rights he has acquired are attached to the content.



This model, which allows people to buy content direct from the rights holder, can also be modified to serve "super-distribution" which is where someone, having enjoyed a digital file, can forward it to a friend (e.g. Frank) who cannot access it until he has replaced the original public key with his own one. This will, of course, involve him in paying the price of the content to the online store.

So far so good, but this is actually where the problems start.

Currently DRM applications are very basic and only scratch the surface of the possibilities. The market for DRM technology is heavily constrained by the lack of an open, scalable and dynamically adaptable solution.

If correctly applied, DRM can be likened to a motorway, providing a seamless high-speed route to content, enabling people to get the content they want, where they want it, quickly and easily. However, if badly applied, heavy handed and overly restrictive, DRM is more like a traffic jam – denying people access to the content they want and crucially denying rights-holders the revenue they want.

A successful DRM system has to be transparent and flexible with the user unaware that DRM processes are going on behind the scenes. However this demands a great deal of co-operation from many different partners, that are managing different aspects of the process, if this is to happen. For the simple purchase of an mp3 track via a mobile phone, this will involve record companies, mobile network operators, billing software providers, handset manufacturers, DRM vendors – all with different priorities, needs and agendas.

An example of how difficult this is, in reality, is provided by the *Open Mobile Alliance*.

Open Mobile Alliance

The Open Mobile Alliance (OMA) was set up members from many different industries, including:

- Mobile phone manufacturers (e.g. Nokia, Motorola, Samsung, Sony-Ericsson, BenQ-Siemens);
- Mobile system manufacturers (e.g. Ericsson, Siemens, Openwave);
- Operators (e.g. Vodafone, O2, Cingular, Deutsche Telekom, Orange) and
- IT companies (e.g. Microsoft, IBM, SUN).

The intention was to set DRM standards for mobile phones.

OMA DRM v1.0

The first implementation of OMA DRM, version 1.0, was approved in June 2004. It is a basic DRM standard which doesn't offer strong protection to content owners. It has been implemented in 400 phones, which may sound a lot until you realize that there have been thousands of different devices released.

However it's the best technology there is for mobile applications at present and many operators use OMA DRM for their content services.

It specifies three main methods:

Forward Lock

Forward Lock prevents the unauthorized transfer of content from one device to another. The intention is to prevent peer-to-peer distribution, or super-distribution, of content using Bluetooth or infrared. The content is packaged inside a DRM message that is delivered to the terminal. The device can play, display, or execute the content, but it cannot forward it.

Combined Delivery

This builds upon the ability to stop super-distribution by allowing the content owners to set rules about how a person may use the content. When the content is delivered to the handset, it contains two objects: the *content* and a *rights object*.

The rights object defines the usage rules for the content. This can support all kinds of functions, such as preview, or time- and usage-based constraints. For example, it allows a complimentary preview, such as using the content only for a specific number of days, or an annual subscription with non-interfering price models.

If a content owner applies the Combined Delivery mechanism, this will ensure that neither the content nor the rights object can be forwarded from the target device.

Thus, on Nokia Series 40 phones, an installed file with DRM will have its "Send" option greyed out in its options menu. If the user attempts to send this via MMS, a message "The file is copyright

Abbreviations

CA	Conditional Access	**OMA**	Open Mobile Alliance http://www.openmobilealliance.org/
CEK	(OMA) Content Encryption Key		
DRM	Digital Rights Management	**PKI**	Public Key Infrastructure
DVB	Digital Video Broadcasting http://www.dvb.org/	**XCP**	(Sony) eXtended Copy Protection

protected" will appear. A Bluetooth file transfer will fail if the user tries to extract the file using Bluetooth, yet the file will still appear as present and will still be deletable via Bluetooth.

Separate Delivery

The most sophisticated level of OMA DRM is called Separate Delivery. It provides better protection for high-value content by encrypting the content itself.

Thus the content is useless without both a rights object and a Content Encryption Key (CEK), which are delivered separately from the content.

The rules set by OMA insist that the CEK is delivered securely, via WAP push, directly to the authorized mobile device. On the handset, the DRM User Agent uses it for content decryption.

OMA DRM-compliant devices such as the Nokia 3200 or 6230, or the Siemens SX1 and C62, store the rights objects in a part of the handset's memory where the user can't see it. Only the handset's media player can access both the encrypted content and the rights object, including the CEK, to enable the consumption of the content by displaying or playing it.

Although people can download content and forward it to friends, they won't be able to see it until they obtain their own CEK for content decryption.

The OMA standards include a "rights refresh" mechanism, allowing people who have had content sent to them by their friends to contact the content owner directly to obtain rights to either preview or purchase the content they have received.

OMA describes this super-distribution as a key benefit of Separate Delivery because it maximizes the number of potential customers through peer-to-peer recommendations while retaining control for the content provider through centralised rights acquisition, potentially triggering enormous revenue growth. It also avoids the distribution costs for rights holders.

OMA DRM v2.0

Having established OMA DRM v1.0, the organization set out to create v2.0 – an open standard for technology to handle the application of DRM to music, video, gaming and similar services delivered to wireless devices – which was approved in March 2006.

OMA describe it as an enhancement on the earlier DRM specification as it is based on the concept of a "trusted terminal", requiring that the handsets support Public-Key Infrastructure (PKI) authentication, which ensures their identity.

The standard includes several control mechanisms built into the handset, allowing for what OMA describe as "a more robust set of content control options".

These benefits include:

- content subscriptions;
- gifting – allowing users to pay for content and forward it to a friend;
- previewing – enabling users to watch a portion of the content before purchasing it, and

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.