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.

EX1055
Roku V. Media Chain
U.S. Patent No. 10,860,691

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.

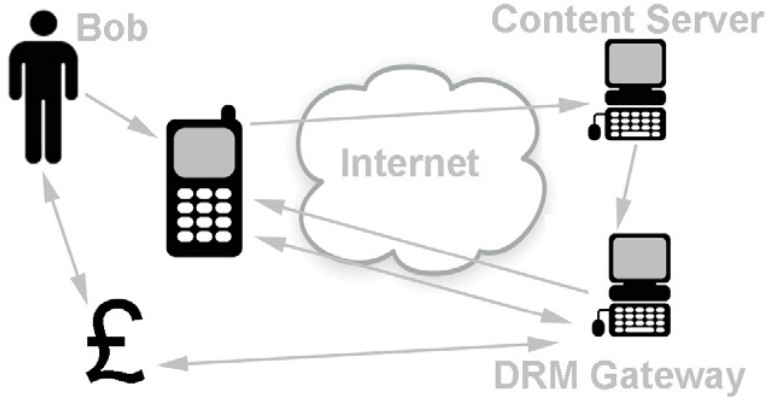
DRM

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

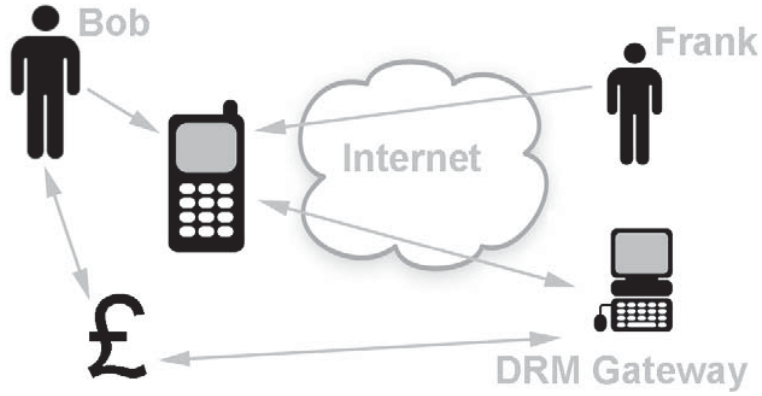
The list of actions covered by DRM are growing even longer, but typically they cover such things as:

- 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	**PKI**	Public Key Infrastructure
DRM	Digital Rights Management	**XCP**	(Sony) eXtended Copy Protection
DVB	Digital Video Broadcasting http://www.dvb.org/		

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

- sharing – the sale of licences that permit the use of content among a set group of wireless devices, and saving the content to memory cards or other compliant devices, among many other new benefits.

Patenting issues

While the first handsets with OMA DRM 2.0 – the Nokia N91 and Sony Ericsson W850i – were put on the market in early 2006, the standard was in the middle of a huge financial row.

The patents necessary to develop the software based on OMA v2.0 are held by MPEG LA. They initially proposed to sell licences at $1 per handset and 1% of every transaction. Obviously this was unacceptable to content owners as it presented them with potentially open-ended bills for DRM fees. MPEG LA eventually now plans to charge $0.65 per handset and $0.25 per mobile phone subscriber per year, still a significant amount, but no longer tied to the number of times the DRM is used. The price cut came after mobile network operators threatened to develop alternative DRM technology, which would have led to a fragmented DRM situation with incompatible files and no clear benefits to anyone.

Apple FairPlay

While the delays and financial arguments over OMA DRM are typical of when several players are involved, when just one organization is dominant it allows a more seamless approach, as is the case with Apple's FairPlay system used on its iTunes store and implemented on its iTunes software and iPod digital music players.

FairPlay allows a track bought from the iTunes store to be used in the following ways:

- The protected track may be copied to any number of iPod portable music players;
- The protected track may be played on up to five (originally three) authorized computers simultaneously;
- The protected track may be copied to a standard Audio CD any number of times. While the resulting CD has no DRM and may be ripped, encoded and distributed like any other CD because it has been compressed, to re-rip it will significantly degrade the sound quality;
- A particular playlist within iTunes containing a protected track can be copied to a CD only up to seven times (originally ten times) before the playlist must be changed.

FairPlay does not affect the ability of the file itself to be copied. It only manages the decryption of the audio content.

Sony rootkit

Some unified vendors unfortunately got their approach to DRM expensively and badly wrong:

> ***"Most people, I think, don't even know what a rootkit is, so why should they care about it?"***

This is a quote that Thomas Hesse, the head of Sony BMG's global digital business, might now regret as, thanks to Sony BMG, many millions of people now know what a rootkit is, and have shown they care quite deeply about it. Furthermore, this approach to DRM has just cost Sony BMG several million dollars to settle class action lawsuits brought by more than 40 US states. The company also faces the prospect of paying up to $175 to many thousands of individual customers under the terms of the legal settlement.

Sony BMG's botched foray into DRM started when they included "eXtended Copy Protection" (XCP) software on music CDs.

When a consumer tried to play a CD with XCP on their computer, they were prompted to install a CD player bundled with the music tracks.

The software on the CD not only prevented the computer's native media player from playing the CD, it also restricted the number of times the CD could be burned and prevented the CD being ripped to the iPod.

These restrictions may have been onerous enough for consumers to object to, but it didn't take long for software engineer Mark Russinovich to realize that this was the tip of an iceberg.

He discovered that Sony BMG's software was fundamentally similar to a rootkit, a programme used by hackers to conceal unauthorised activity on computer systems, often described as Spyware or Malware. Thus, without the consumers' explicit knowledge or permission, Sony BMG had installed software on their computers that interfered with the normal way in which Microsoft Windows or Mac OS X operating systems play CDs and it opened security holes that allowed viruses to break in. Furthermore the software caused programmes to freeze up and applications to slow down: a series of hidden files that were the source of the problem proved to be nearly impossible to uninstall.

Russinovich published his findings on his blog and the story was quickly picked up by the mainstream media, leading to several class-action lawsuits against Sony BMG, and even criticism from some Sony artists that their work had been protected by methods they didn't approve of.

Although Sony BMG quickly released an uninstaller, this too was fundamentally compromised. Not only did users have to provide their e-mail address, which Sony BMG reserved the right to use in future marketing activities, the procedure for obtaining the uninstaller was complicated and time-consuming and would only work on one computer each time. If a user had played the CD on several computers they had to go through the process several times.

The uninstaller also used Microsoft's ActiveX controls which many security experts recommend that people de-activate, as it may allow malicious attackers to take over control of people's computers.

Sony BMG's final indignity came when they were criticised by the US Department of Homeland Security:

> *"It's very important to remember that it's your intellectual property — it's not your computer's",* Stewart Baker, the assistant secretary for policy, told the Washington Post. *"And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."*

Sony BMG eventually recalled all unsold CDs with XCP and offered to exchange CDs that people had bought for ones without the software. In December 2006, Sony BMG agreed to pay damages and fines to settle lawsuits brought by more than 40 US states. The company will pay Texas and California $750,000 in civil penalties and costs, and $4.25m to a consortium of other states as well as reimbursing consumers up to $175 each if their computers were damaged while trying to uninstall the XCP software.

A growing movement against DRM

Sony BMG's sorry tale is perhaps the most extreme, but is by no means the only example of major criticisms being levelled at DRM.

There's a growing movement against DRM. While Defective by Design's *Day Against DRM* on 3 October 2006 hardly made the mainstream news agenda, perhaps a more significant announce-

ment the same week came from UK nightclub group, ***The Ministry of Sound*** (MoS). In an article in *The Times* on 2 October 2006, they announced that they were starting an online music store with 60,000 tracks which would be DRM-free.

Lohan Presencer, managing director of the MoS Group, was quoted as saying: *"DRM is a nonsense. It only succeeds in limiting choice and people still steal music regardless."*

As The Ministry of Sound is the UK's largest independent record company, selling about 2 million compilation dance CDs a year, and operates an international chain of "super-clubs", they are one of the most significant companies so far to reject DRM.

eMusic is another music download site which does not feature DRM and has a 13% market share in the USA. It recently launched in Europe with a catalogue of 1.7 million tracks from 8,500 independent labels.

The major advantage touted by both these services is that because they sell mp3s without DRM, their tracks can be played on any digital music player, computer or HiFi system.

iTunes may have the dominant share of paid-for music downloads worldwide, but an intentional limitation of it's DRM system, FairPlay, is that it prevents iTunes' customers from using the purchased music on any portable digital music player other than the iPod. This is one of the major criticisms of proprietary DRM systems that, instead of protecting intellectual property, they are in fact locking consumers into a single technology platform.

And further problems are becoming evident in the growing VoD. market. Apple users are currently locked out of many new services such as the one just launched by Channel 4 in the UK

That's because Apple has chosen not to licence FairPlay to other companies, hoping that content owners will instead use their iTunes platform to distribute their content. However this presents a problem for content owners such as C4, whose brand is big enough to justify building their own D2C portal. If they see iTunes as a rival and are reluctant to use it to distribute their programmes, their only option if they want to protect their content is to use Windows Media DRM which only works on PCs. Is the solution here for Microsoft to develop Windows DRM that works on Macs?

Technical innovation and artistic creativity

The debate is only going to get more intense as the US content industries make a second attempt the get the ***Broadcast Flag*** technology through Congress. This will insert a digital "watermark" into a broadcast stream which will control whether or not it can be recorded, or impose restrictions on what can be done with the recording. Ultimately this will restrict viewing of "flagged" content to devices which are compliant, forcing consumers to upgrade their technology to compliant devices, or miss out.

A similar debate is happening in Europe where the DVB Project is attempting to get its ***Copy Protection and Content Management*** (CPCM) standard included in the next EU Copyright Directive. This is actually regarded as a more onerous series of restrictions than the US broadcast flag and will finely control which devices can be used to view programmes. As it contains a "robustness requirement" that prevents the end user from modifying the receiving device, it will be impossible to use open-source software such as Linux to create receiving devices.

This will have a profound effect on the European set-top box market as most manufacturers use Linux as their operating system.

This illustrates one of the unintended side-effects of DRM, that it restricts ***technical innovation***.

Opponents of DRM argue that the iPod would never have been invented if DRM had been present on audio CDs. It's likely that one of the restrictions that would have been in place would have been to only allow audio output to a "trusted" pair of loudspeakers. Thus when CD drives started appearing in computers, users would not have been allowed to extract the digital data, i.e. rip them to mp3s, unless the content industry had given permission, which seems unlikely. So people would not have started storing their music collection as mp3s, there would have been no need to develop portable mp3 players and a whole industry would never have arisen.

While some copyright owners might not regard this as a bad thing, acts like the Arctic Monkeys and Gnarls Barkley that have grown through file sharing and file downloading would most likely disagree.

It's not just technical creativity that is compromised, ***artistic creativity*** is also hindered. The restrictions imposed by FairPlay mean that a track bought from the iTunes record store cannot be imported into any digital editing systems. So if someone editing together their holiday video and wanting to run a track bought from iTunes under some of their shots will find they're unable to.

And while this may be a minor irritation to home video enthusiasts, there are potentially wider cultural implications. Throughout history, artists and composers have developed through being influenced by or even copying other artists. This article started with the example of Mozart copying Allegri's *Miserere*, but Bach is also widely credited as an important influence on Mozart, just as Mozart himself went on to influence dozens of other composers.

The process continues in the digital age. Over the last few years, artists such as The Kleptones have created albums by remixing, or mashing-up, tracks from dozens of artists along with clips from films and TV programmes, creating a new art-form in the process.

The restriction on importing tracks bought from iTunes into video-editing software could also contravene a consumer's long-held rights. In many countries, copyright includes ***the principle of fair use***. While this does not allow wholesale copying of a copyrighted work without the owner's consent, it does allow limited quoting. So inserting a clip from a song into a documentary about music, or into an individual's holiday video would usually be considered as fair use.

Also compromised by DRM is ***the doctrine of first sale***. This means that if you have purchased a licence to a copyrighted work, you have the right to sell that licence to someone else. But a digital file with DRM applied prevents this, so if I buy an album from iTunes and I don't like it, I can't then sell it on eBay as I would if I bought a CD I didn't like.

Battery consumption

A further objection to DRM, especially where handheld devices are concerned, is over the extra power consumed by the software.

The website MP3.com tested the battery life of mp3 players, intending to discover how close their actual battery life came to the manufacturers' specs. They were also looking to find out what sort of things drained the power more quickly. They weren't surprised to find that attaching a chunky "DJ-look" pair of headphones, or watching videos, quickly drained the batteries but they also discovered that restricting songs with DRM can significantly reduce the battery life.

The batteries in a Creative Zen Vision:M lasted for 16 hours when playing mp3s, but when used to play WMA subscription tracks, they only lasted just over 12 hours, a drop of 25%. It was the same with other PlaysForSure players such as the Archos Gmini 402 Camcorder which lasted 11 hours, with mp3s but only 9 hours with DRM tracks.

Considering that one of the biggest complaints about handheld media players is the battery life, which is only going to get more acute as new wireless technologies are added and more rich-media content is used, something that reduces the effective battery by 25% is a huge issue.

Richard Leeming has been working on interactive broadcast content for nearly 10 years. After being one of the BBC's first interactive content producers, he joined Red Bee Media in 2002 to help set up the Content Factory, running a team which manages, creates and publishes content for 3, the UK 3G network. In his current position as Business Development Manager – Interactive Content, he is responsible for working with Red Bee Media's clients to help them understand how to develop products and services for the Mobile Content Market.

Mr Leeming's understanding of interactive content draws on his career as a broadcast journalist for the BBC, working for programmes like the *Today* programme on Radio 4, *Breakfast* and *Drivetime* on Radio 5 and *Newsbeat* on Radio 1.

So it would seem sensible then for all players in the digital media market to start moving towards some kind of consensus on DRM. Some hard questions need to be asked, and some difficult answers arrived at.

Conclusions

Is it really sound business practice to treat your consumers like thieves? Or to install spyware on their computer without them realizing it?

In an era where, in politics, choice is everything and we go to war over freedom, is it beneficial to the bottom-line for the digital media industry to be so actively seeking to restrict people's choice and freedoms over what they watch and listen to?

We need to start thinking hard about when and how we apply DRM. At IBC's *Multimedia on the Move* Tutorial in September 2006, Martin Coggin of BT Movio insisted that, because their Virgin Lobster DMB receiver had a hard disc, could function as a PVR and could sync to a PC, then DRM was absolutely necessary. I found myself wondering – given the quality of the pictures, the size of the screen and the inherent usability issues of a mobile phone – how many people were going to go to the trouble of pirating content from the BT Movio service? This shouldn't in any way be regarded as a criticism of the BT Movio service, just a recognition that there are some services where DRM gets in the way.

If we regard mobile TV as a promotional service to drive consumers to higher-value broadcast services where the returns are greater, then surely allowing people to distribute the service virally increases the uptake and reduces the distribution costs.

Clearly this doesn't hold for all content. High-value, short-form content such as music videos or sports clips have much greater attraction for pirates and so DRM is vital, but maybe the digital content industry could consider the "Economics of Trust"?

In North London there is a restaurant called "Just Around The Corner". There are no prices on the menu, people pay what they think is fair. In fact, if they pay less than what the owner thinks is fair, then he thanks them politely and returns their money. The restaurant has been running for 17 years so surely illustrates that if you play to individual people's better nature, then you will be rewarded.