



GiantSteps
Media Technology Strategies

250 West 57th Street, Suite 2017
New York NY 10107
212 956 1045
fax: 212 581 1352
www.giantstepsmts.com

Digital Rights and Digital Television

Originally prepared for the symposium *Digital Television: Beyond HD & DTV* at The Columbia University Institute for Tele-Information at Columbia Business School, November 2, 2007.

By Bill Rosenblatt

March 31, 2009

© 2009 GiantSteps Media Technology Strategies. All trademarks are the property of their respective owners.


 This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivative Works 3.0 United States License. For more information, see <http://creativecommons.org/licenses/by-nc-nd/3.0/us/>.

Table of Contents

Table of Contents	2
Abstract	3
Introduction	3
Purposes of Digital Rights Technologies	4
Types of Digital Rights Technologies.....	6
DRM	6
Digital Watermarking.....	6
Fingerprinting.....	7
Rights Information Management	8
DRM for Digital Television.....	9
Transmitter to Gateway Device	9
Gateway Device to Home Network	10
Axes of DRM Power in the Digital Home	10
The Internet and User-Generated Content.....	13
The DRM Tug-of-War.....	15
About the Author.....	18
About GiantSteps Media Technology Strategies	18

Abstract

As the media industry struggles with the large-scale copyright infringement made possible by networked digital media, one of the most interesting – and most controversial – aspects of digital content distribution is control over content rights. In this paper, we examine the state of the market for digital rights technologies specifically for digital television and other manifestations of digital video. We also discuss the relationship between digital rights technologies and certain aspects of copyright law.

This white paper is an updated version of a paper originally prepared for the symposium *Digital Television: Beyond HD & DTV* at The Columbia University Institute for Tele-Information at Columbia Business School, November 2, 2007¹. The paper was published as a chapter in the book *Television Goes Digital* (New York: Springer Science + Business Media, 2009)².

Introduction

In late 1993, an ad-hoc collection of academics, technologists, publishers, and policy wonks came together in Washington, DC, for a conference called *Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment*³. The conference organizers were prescient in that they understood intuitively that the digital content revolution would in large part be about rights.

But the proceedings from this conference show – in 20/20 hindsight – a bunch of blind men attempting to describe the unseen elephant that they know is in the room. Few could truly foresee how markets for online content would develop and how technologies for both distributing content and controlling rights would develop along with them.

The world has changed a lot in the last 15 years, and yet with respect to the problems of rights management, it hasn't changed that much: the essential problems that content owners face when distributing their content in digital form persist. Bits are still easy to copy; the Internet is still essentially an open architecture; and many types of content rights are still accounted for with blunt instruments such as statistical sampling and blanket licensing.

The challenges associated with content rights for digital television are fundamentally no different from those associated with digital music, e-books, and other digitized media. Digital television (generally speaking) adds a few layers of complexity compared to other types of content, but the inter-industry dynamics, market forces, and interfaces between law and technology remain substantially the same.

¹ Program available at <http://www4.gsb.columbia.edu/citi/events/eventsarchive/digitalviptv>.

² Available online at <http://www.springer.com/business/media-management/book/978-0-387-79977-3>.

³ Proceedings still available at <http://www.cni.org/docs/ima.ip-workshop/>.

Purposes of Digital Rights Technologies

Technologies for controlling and tracking content usage are not new; they have been around for centuries. The physical characteristics of traditional media products serve as de facto “rights management technologies.” Consider the printed book: books are easy to give and lend; they can be read by only one or two people at a time; they can be copied with some effort and expense; they are difficult to alter without detection. This “rights management” has been implicit in book industry business models for a very long time.

Early electronic media also had “rights management” attached to it, such as plastic “do not record” tabs on audio cassette tapes and serial copy management on VHS videotapes. Even some digital media products distributed physically, such as DVDs, are encrypted.

Of course, the more recent availability of “pure” digital files and the ascendancy of open-access data networks such as the Internet have changed the game. These factors have shifted the balance between content owners and consumers so that the latter have much more power to use content in ways not contemplated by the owners and, in many cases, not permitted by law. As commercial content providers began to grapple with this monumental shift, technology vendors began to offer ways to approximate the physical limitations on content use, that have been present for all these years. Thus the notion of digital rights management (DRM) was born.

As the market for digital content technology has developed over the past decade-plus, however, other purposes for digital rights technologies have emerged along side those emulating physical media usage constraints. These primary purposes are as follows:

- **Curb misuse of content.** We use the term “misuse” intentionally to cover both uses that are not permitted by copyright law and those that are not permitted by the licenses that consumers agree to abide by for content usage under digital distribution schemes. There is a current debate over whether pure digital distribution of content is governed by copyright law. Content owners generally hold that it is instead governed by license terms, often of the “clickwrap” variety⁴. We also use the term “curb” advisedly as the content industries have abandoned the notion that DRM can completely prevent misuse. This newer view of DRM is as a series of “speed bumps” intended to make misuse more trouble than it’s worth.
- **Enable new content business models.** Control over content access is thought to be necessary to enable multiple offers that lead to efficient markets⁵. In the digital realm, there are virtually no limits on new business models that can be created, though some of these are not feasible without digital rights technologies. The most prominent example of this is subscription services, such as Rhapsody for music or CinemaNow for movies and TV. In these, a user pays a monthly or annual subscription fee and gets on-demand access to any content in the services’ subscription libraries. This model resembles neither of the two predominant legacy distribution models: physical products (CDs, DVDs) or

⁴ For example, Twentieth Century Fox refers to “download-to-own” Internet video distribution as “electronic licensing” rather than the more standard industry term “electronic sell-through” because the latter connotes sale of a copyrighted work, which could be interpreted as subject to copyright law.

⁵ Einhorn, Michael and Bill Rosenblatt, *Peer-to-Peer Networking and Digital Rights Management: How Market Tools Can Solve Copyright Problems*. Cato Institute Policy Analysis No. 534, 2005.
http://www.cato.org/pub_display.php?pub_id=3670

broadcasting. Digital rights technology is needed to prevent a user from signing up for the service, paying for one month (or not), copying every item in the library, and then canceling. Another example is advertising-based services like QTrax, in which users can download and listen to music as much as they want for free as long as they view ads on a periodic basis – i.e., limited rights to content in exchange for non-financial consideration.

- **Track content usage.** Digital rights technologies can be used to track consumers' use of content, not to limit their usage rights but to provide inputs to schemes for compensating rights holders. The use of digital rights technologies for this purpose is not yet widespread⁶, but similar technologies are currently used by media ratings agencies such as Nielsen to track content viewership for advertising rate-setting purposes.
- **Lock consumers into technology platforms.** As we will see shortly, technology vendors need incentives to offset the cost of incorporating digital rights technologies into their products and services. A powerful incentive for any technology vendor is that of consumer lock-in⁷. The most prominent – but by no means only – example of this is Apple's iTunes, which has used FairPlay DRM to lock consumers in to the iPod for both audio and video content.

⁶ A technology called Broadcast Monitoring emerged during the first Internet Bubble that used digital watermarks to track music plays on radio. After some limited experimentation, this technology did not succeed in the market. Instead, traditional inaccurate methods of compensating music rights holders for radio airplay, such as statistical proxies, survive, while at this writing new attempts are being made to revive broadcast monitoring, this time with video content.

⁷ See generally Shapiro, Carl and Hal R. Varian, *Information Rules*. Cambridge, MA: Harvard Business School Press, 1999.

Types of Digital Rights Technologies

The term DRM has a range of meanings. The narrower definition refers to technology that encrypts content and requires special hardware or software to decrypt it and allow the user to exercise rights, such as play or copy. This is the definition most commonly used in the press.

The broader definition encompasses any technology used to control, track, or manage use of digital content. We acquiesce to the use of DRM in the narrower sense and use the term “digital rights technologies” for the broader meaning. There are four basic types of digital rights technologies.

DRM

A “classic” DRM system⁸ generally has the following components:

- A *content packager* that runs on a server, typically that of a content retailer. The packager encrypts the content along with some metadata (information about the content).
- A *license server* that also runs on a server. A license server processes requests from the user’s software or device to obtain rights to encrypted content. It checks credentials, including the identity of the user and/or device, and if valid, creates a small encrypted file called a *license* and sends it to the user’s software or device. The license contains content encryption keys and possibly a description of the rights granted.
- Functionality on the user’s device to process content usage requests, communicate with the license server to obtain a license; decrypt the license; extract content encryption keys and rights; and exercise the user’s rights. Often this functionality is part of a media player such as iTunes (FairPlay DRM) or Microsoft Windows Media Player (Windows Media DRM).

Digital Watermarking

Digital watermarking refers to embedding data into content in such a way that the user does not perceive it⁹. Digital still images, audio, and video can be watermarked. Watermarking technologies have two parts: insertion (or embedding) and detection (or extraction).

Watermarking schemes are designed so as to trade off among several qualities, including:

- **Capacity:** the amount of data that can be embedded.
- **Robustness:** the ability of the watermark to survive file format conversion, digital to analog conversion, downsampling, etc.

⁸ See for example Rosenblatt, B. et al, *Digital Rights Management: Business and Technology*. New York: John Wiley & Sons, 2001, Chapter 5.

⁹ Some watermarks are meant to be visible or audible in order to act as a deterrent to misuse. For example, samples of digital images that are not meant to be used in production typically contain visible marks identifying their sources.

- **Undetectability:** lack of effect on the user's perception of the content.
- **Security:** imperviousness to removal or alteration.
- **Efficiency:** speed of insertion and detection.

The data included in an imperceptible watermark is generally limited to a few dozen bytes. But that information can be anything, including the identity of the content owner or that of the user or device that downloaded it. Often a watermark is an ID number that is looked up in a database for further information about the content.

Watermarks can be used for forensic tracking of content as it makes its way through cyberspace; examples of this include Activated Content's watermarking scheme for pre-release music and Nielsen's Digital Media Manager for television content distributed on the Internet. They can also be used to take actions according to the identity of the content, such as serve a contextually related ad to the user or compensate rights holders; such business models are often discussed but are not yet common in real life.

Fingerprinting

Fingerprinting refers to examining the data in a content file and calculating a set of numbers that represent its characteristics (the content's "fingerprint"), then looking those numbers up in a database to determine the content's identity. Audio and video can be fingerprinted.

The fingerprinting technique for music was first proposed around the time of the *A&M v Napster* litigation in 2001, when the file-sharing service was searching for ways to control the use of copyrighted material that satisfied the court¹⁰. The most common use of fingerprints is to block uploads of copyrighted files to file-sharing networks; the iMesh peer-to-peer (P2P) network began to use audio fingerprinting in 2005, with the blessing of the major music companies, for this purpose.

User-generated video content (UGC) sites like YouTube and MySpace are also using audio fingerprinting to block unauthorized content, such as music videos. More recently, the social networking site imeem is using it to serve contextual ads to users who upload music files and send a portion of the ad revenue generated to rights holders. Auditude is building something similar for video content.

Fingerprinting for video is a newer technique, considered by many to be experimental at this stage. Digital video is far more complex to analyze than audio. The primary applicability of video fingerprinting at this point is for UGC sites; see below.

Fingerprinting and watermarking are sometimes known collectively as *content identification*. There is some overlap between viable applications for the two technologies, but there are also important differences:

- Watermarking requires that some entity in the content value chain – content owner, distributor, retailer, or end-user device – insert watermarks into content files. Fingerprinting requires no analogous effort.

¹⁰ Napster and Relatable Enter into Agreement, Relatable Inc. press release, April 20, 2001, <http://www.relatable.com/news/pressreleases/010420.release.html>. Napster never did launch its paid service and thus never put Relatable's audio fingerprinting technology into production. The service called "Napster" today has the same brand name but completely different technology.

- Fingerprinting is not one hundred percent accurate at identifying content. Watermarking is, by definition¹¹.

Different copies of a given work can have different watermarks: for example, watermarks denoting the retailer where the file was purchased or the user who downloaded it, or watermarks denoting the version of the content (e.g., North American vs. UK). In contrast, a given work always has the same fingerprint (provided that the fingerprinting technology works properly).

Rights Information Management

The final digital rights technology is one that is (or ought to be) used within media companies rather than in distributing media to the public. It is desirable to track information about content rights holders, the rights that a company has to their content, rights that the company can pass on to third parties, the terms under which that can be done, and so on.

This can be very complex information to manage, but doing so makes it easier to create content licensing deals, compensate rights holders, and mitigate legal risk. Some media companies have built customized databases to track rights information, while others have adopted off-the-shelf systems from a handful of vendors. Such systems can integrate with other systems within media companies, such as financial, ERP (enterprise resource planning), and royalties. Ideally, they can also integrate with digital rights technologies for consumer content distribution.

¹¹ Assuming that the content has not been altered so much that watermark detection becomes difficult or impossible.

DRM for Digital Television

In this section, we examine DRM and related technologies specifically for digital television. These break down into two parts:

- Technologies used to protect content from the transmitter or distributor to the consumer's gateway device, which could be a set-top box (STB), PC, etc.
- Technologies used to protect content from the gateway device to other devices in the consumer's home or personal network.

We also discuss how digital rights technologies – particularly content identification technologies – are being used with user-generated content sites.

Transmitter to Gateway Device

In general, digital television schemes feature some sort of a transmitter sending content to a consumer device. The transmitter could be a digital broadcaster, cable head end, satellite, or Internet server.

The basic concepts in protecting the link between the transmitter and the consumer's gateway device are to encrypt content over the link and pass along rights information. The latter is often taken from a subscriber management system; it can include identities of users or devices that are entitled to content rights, as well as descriptions of those rights. One example of such rights could be “allow the user to play this content for up to 48 hours.”

This type of technology can be thought of as a successor to traditional conditional access (CA) systems for analog cable television. CA systems descramble content on the user's device. In many CA systems, the user plugs a SmartCard into the STB, which provides a credential to decrypt the content. This is like a simple DRM system that supports a single right, that of “play this content right now.”

More modern technologies of this nature are used with digital cable, satellite, and IPTV. An early technology from Widevine replaced physical SmartCards with a software solution, which eliminated the cost and logistical complexity of distributing SmartCards; subsequent technologies added the ability to process more sophisticated rights.

In addition, many modern technologies incorporate digital watermarking in addition to encryption, one examples being Verimatrix's VCAS system. In many cases, the type of watermarking used in this scenario is known as *transactional watermarking*, in which the identity of the client device (e.g., STB) is embedded into the content as a watermark at transmission time. This enables content to be traced forensically to the user who downloaded it if it is found in an unauthorized place, such as a file-sharing network.

An important criterion for technologies that encrypt digital television signals from transmitters to STBs is that they minimize the amount of extra hardware required on the STB. This encourages adoption of the digital rights technology by STB vendors, which in turn makes it more attractive to digital TV service providers, who distribute STBs to users.

Gateway Device to Home Network

The DRM-related technologies for digital television inside the home are far more complex and varied. They relate to the essential idea that consumers should be able to use legitimately obtained content anywhere in their home – or on any device in a *home network* or *personal network*, which theoretically includes portable and automotive devices. Many content owners have generally come to accept this idea and thus have evolved their attitudes from insisting that consumers pay separately for each version of content for different devices.

This more tolerant attitude aligns with that of much of the consumer electronics industry, which sees the digitally connected home as the next great opportunity to sell new gadgets to consumers. From the DRM perspective, digital home architectures include a “control center” device, which functions as both a gateway device (in the sense described above) and as the controller of how content can be sent around to various other devices connected to the network. The boundaries of the network – often referred to as a *domain* – can be expressed as a maximum number of devices or all devices within a certain distance from the control center¹².

Axes of DRM Power in the Digital Home

Thus the market for DRM for home media networks can be seen as a struggle among various factions for ownership of the crucial control center. The owner of the technology platform for the control center can then dictate which devices can play on the network and under what conditions (e.g., by licensing technology from the control center platform providers).

The factionalism in this market is not among individual technology vendors; instead, the market has coalesced into ecosystems, or “axes of power,” based on device types. Each axis has DRM technologies that the members of the axis are attempting to assert as standards. It should be apparent how DRM is a strategic tool for technology platform owners to achieve lock-in, as described above.

The four axes of DRM power in the digital home are:

1. Set-top box (STB) axis
2. Media player axis
3. Mobile handset axis
4. PC axis

Apple may constitute a fifth axis of power if it either opens its platform to third-party vendors or produces more (or more successful) products for the digital home.

Each of these axes of power is represented by a group of technology vendors and a DRM technology that is either proprietary or based on a specification from a standards body or consortium. Some vendors will participate in multiple axes. We now examine each of these axes of power.

¹² As measured by the length of time it takes for a signal to roundtrip from the control center to the device and back; this allows for wireless network connections.

The Set-Top Box Axis

The STB axis includes these vendors:

- **STB vendors:** Pace Micro, Humax, Maxian, ADB, Amstrad, Pace Micro, others
- **Incumbent CA technology vendors:** Thomson, NDS.
- **Semiconductor makers:** AMD, ARM, ATI, Broadcom, Conexant, STMicroelectronics, Texas Instruments

The DRM technology for the STB axis until about 2007 was Secure Video Processor (www.svpalliance.org), a consortium that was started by NDS and Thomson in 2004. SVP enables content providers to set relatively simple rules for how content can be used in a home network once it reaches a STB. The complexity of SVP has been kept fairly low in order to minimize the incremental cost of hardware on STBs that support it. The SVP Alliance had members other than the above companies, including major consumer electronics companies such as LG Electronics, Samsung, and Philips¹³.

After semiconductor makers STMicroelectronics and Broadcom introduced chips that implemented SVP, some STB makers adopted those chips in their designs. However, at this writing, SVP appears to be stalled. A number of STB vendors are using Marlin (see below) for IPTV implementations, especially in certain Asia-Pacific markets.

The Media Player Axis

The Media Player axis's major players are Sony, Philips, Panasonic (Matsushita Electric Co.) and Samsung. The other major player is Intertrust Technologies, a DRM research and development company that holds many core DRM patents and is now owned jointly by Sony and Philips.

The DRM technology for the Media Player axis is Marlin (www.marlin-community.com). Marlin is a consortium-based technology whose primary inventor is Intertrust. The initiative was announced in early 2005, and it released its first spec the following year. Marlin is nominally intended for portable (or non-portable) media player devices that can connect to a network.

Users register with an online service as owners of Marlin-based devices; they also register with services as purchasers, subscribers, or other obtainers of content. When such a device receives content to copy or play, Marlin goes through a process of tracing conceptual links¹⁴ from the user's identity through devices and services to the content, in order to ensure that the user does have the right to use the content.

Trials of Marlin took place in Japan in 2007 for IPTV to Internet-enabled television sets; now most new IPTV-enabled STBs in the Japanese market support Marlin. Pioneer Electronics launched a Marlin-powered service in the United States through a spinoff company called SyncTV in late 2007; Intertrust acquired SyncTV in February 2009. Sony has incorporated Marlin into PlayStation gaming systems and the Sony Reader device for e-books.

¹³ One major content owner, Twentieth Century Fox, is also a member of SVP. However, this could be viewed as an extension of NDS's involvement: Fox and NDS are siblings in the News Corp. family.

¹⁴ More specifically, Marlin uses standard concepts from directed graph theory.

The Mobile Handset Axis

The Mobile Handset axis has some obvious overlap with the media player axis; there are several vendors that are involved in both. As far as DRM is concerned, Nokia has been the nominal leader of this axis.

The handset axis's DRM strategy is based on a DRM standard from the Open Mobile Alliance, a pre-existing standards body that also creates and maintains standards in many other areas of mobile telecommunications.

There are two major versions of Open Mobile Alliance DRM (OMA DRM) – 1.0 and 2.0 – and they are very different. OMA DRM 1.0, released in 2002, is not relevant to home media networks; it was designed for low-end handsets with built-in media players but not much computational power. Its low cost of implementation has led to an installed base of over half a billion devices, though only a fraction of those are actually used with any OMA DRM 1.0-compatible content service.

OMA DRM 2.0 is a much more powerful and flexible DRM scheme that can support rich media, including digital video. It is capable of supporting a range of rights equivalent to DRM schemes for PCs, like Windows Media DRM from Microsoft. It has some hooks for home network applicability, such as the ability to use domain authentication – i.e., to allow the use of content on all devices in a domain (personal or home network), as described above.

Although OMA DRM 2.0 has been around since 2004, it has gotten relatively little uptake in the market so far, the highest-profile being the BBC's iPlayer with certain Nokia handset models. One of the obstacles has been contention over royalties from DRM patents held by Intertrust and other companies. At this writing, OMA DRM 2.0 is expected to gain traction in mobile TV broadcasting, e.g., together with the DVB-H standard in Europe.

The PC Axis

Microsoft, not surprisingly, sits at the center of the PC axis, which is based on the idea of the Windows Media Center PC as the control center device. The DRM for the PC axis has been Microsoft Windows Media DRM (WM DRM).

WM DRM started out around 2000-2001 as a DRM scheme solely for Windows PCs. With Version 10, introduced in 2004, Microsoft introduced WM DRM for Network Devices, a DRM technology that supports home media networks. Another important technology in the Microsoft platform is Microsoft Media Transfer Protocol (MMTP), which enables secure transmission of content from one device to another.

With WM DRM 10, Microsoft also introduced the ability for makers of non-Windows devices to license the technology, along with a "logo program" called PlaysForSure (www.playsforsure.com) that signifies WM DRM compliance. The semiconductor makers Cirrus Logic, Portal Player, and Sigmatal have embedded WM DRM into their chipsets for consumer devices.

As a result, the WM DRM ecosystem includes a large number of hardware makers, not just PC vendors like Dell and HP. Most of these are portable device makers (Archos, Audiovox, Creative Labs, iRiver, Rio, Samsung, Sandisk, etc.), but some are makers of devices for the digital home such as Denon, Digitrex, D-Link, Netgear, Pioneer, and Roku,

whose WM DRM-compliant products include streaming media servers, audiovisual receivers, flat-panel TVs, and adapters for existing television sets.

Unlike SVP, Marlin, and OMA DRM 2.0, there are currently many content services that use WM DRM. It is possible to obtain video downloads in Windows Media format from services like Movielink (Block buster) and CinemaNow, and transfer them to other WM DRM-compatible devices in the home as well as to standard TVs through adapters.

In 2008, Microsoft introduced a new DRM called PlayReady, which is primarily intended for the mobile market as a competitor to OMA DRM 2.0 and Marlin. Yet Microsoft still supports WM DRM 10.

Apple

Apple is the wildcard in the digital home arena. The company has a strategy for digital home media networks, but it is much different from the others. Instead of putting a platform based on products and/or published specs out in the market and trying to attract a critical mass of vendors, it is sticking to its usual strategy of only releasing its own products and not licensing its technology to third parties. iTunes, video-playing iPods, and Apple TV are its products for digital video.

Apple's DRM, FairPlay, is a rudimentary technology compared with the others described here. Apple licensed it in 2001 from a small company called Veridisc that has since disappeared. It has no ability, for example, to represent different types of rights that are being granted to devices or users; support for specific rights must be "hard wired" into surrounding technology such as software for iTunes, iPods, and Apple TV devices.

Apple built the ability to offer time-bounded content rights in to the latest generation of iPods, Apple TV, and iTunes in order to support a 24-hour movie rental service that it launched in January 2008. In this service, movies can reside only on a single device at a time (regardless of how many devices the user owns), and the software deletes each file 24 hours after the user starts the first play.

As we will see shortly, Apple's strategy for the digital home may look hesitant and tentative compared with the others, but there is a strategic reason for that.

As a final comment on the axes of power, it's worth noting that four or five is too many. Most technology markets settle down to one or two dominant vendors, surrounded by a handful of niche players¹⁵. Although these axes of power represent distinct markets, convergence will lead inevitably to consolidation of DRM strategies.

The Internet and User-Generated Content

The foregoing two-part scenario pertains to content distribution systems that involve servers, gateway devices, and other client devices. But alongside this broadcasting-derived paradigm, there is a huge groundswell of activity around websites that feature user-generated content (UGC), such as YouTube, DailyMotion, and Veoh.

As mentioned above, most creators of so-called user-generated content are not interested in protecting their revenue opportunities (many are not interested in direct revenue at all).

¹⁵ See generally Moore, Geoffrey A., *Crossing the Chasm*. New York: HarperCollins, 1991. In his terminology, these vendors are "gorillas" and "chimps" respectively.

Yet a lot of copyrighted material from major media companies ends up on these websites, so the media industry has been trying to figure out how to either block such content or monetize its appearance on UGC sites.

“Classic” encryption-based DRM is a nonstarter in this scenario, because the vast majority of content creators who post content on UGC sites would not be interested in it. So the media industry is increasingly turning to content identification technologies – watermarking and fingerprinting – as its putative solution.

Content identification technologies serve a very practical purpose in this case: they enable media companies to avoid spending untold time and money in scouring these websites for their content and issuing so-called takedown notices¹⁶. Instead, UGC sites can use content identification technologies to block unauthorized uploads of copyrighted material, or to apply business rules to uploads, e.g., display a targeted ad to the uploading user and give the content owner a piece of the ad revenue. This has two advantages as far as content owners are concerned: it shifts the cost burden to the UGC site operator, and it enables content to be blocked before the damage is done.

Currently, fingerprinting is the preferred content identification technology because it requires the least amount of effort from content owners and other players, though watermarking solutions are being developed. Video fingerprinting technologies have emerged over the last couple of years from several vendors.

It is fair to say that Hollywood views video fingerprinting as the “silver bullet” solution to its problems with UGC sites, despite the fact that the technology has yet to be tested very extensively in the real world. MovieLabs, the R&D joint venture of the major film studios, held a closely-watched competition of video fingerprinting technologies in September 2007. A dozen vendors participated; MovieLabs has kept the results confidential, in part because they were lab tests and do not necessarily reflect real-world behaviors.

Furthermore, Hollywood got together with several leading UGC sites in October 2007 and created a document called User Generated Content Principles¹⁷ – a sort of “peace treaty” stipulating that movie studios and television networks would not sue UGC sites if they implemented content identification technologies in good faith. One company that is conspicuously absent from the UGC Principles is YouTube (Google), which is being sued by Viacom over this issue. On the other hand, while Viacom is participating, Time Warner and Sony Pictures are conspicuously absent on the content owner side.

The UGC Principles document carefully allows for both watermarking and fingerprinting technologies to be used in identifying content. So far, the only entity that is implementing a watermarking-based solution for UGC sites is Nielsen, which is working with the watermarking technology company Digimarc. Yet even Nielsen’s Digital Media Manager solution employs video fingerprinting in cases where the technology cannot detect a watermark in a video file.

¹⁶ By law, specifically 17 USC 512 in the United States, network service providers are obligated to remove content on receipt of takedown notices that contain the required information.

¹⁷ <http://www.ugcprinciples.com/>.

The DRM Tug-of-War

In many respects, and despite the massive popularity of YouTube and other video UGC sites, the UGC scene is currently a sideshow to the current focuses of the media and electronics industries. Not far off in the background while the CE axes of power vie for supremacy is the essential conundrum of DRM, a tug-of-war among three factions: the consumer electronics and IT industry (taken as a whole), the media industry, and consumers.

The media industry has the primary incentive to promote the use of DRM. It has been fighting a battle against copyright infringement that gets more and more difficult with new technologies. The industry's approach to anti-piracy has been one of "fight the battle on all fronts" – including law, technology, and consumer education – with relatively little coordination among the different approaches and even less attention paid to their relative effectiveness or economic efficiencies¹⁸.

Major content owners typically require that content distribution services adopt approved digital rights technologies as a condition of granting content licenses, while smaller "indie" content owners do not. The best way to explain this dichotomy is to note that content from major studios often comes from "brand name" creators and thus already has a market; studios seek direct revenue from such content. In contrast, indie content owners seek exposure and are thus predisposed to trade off revenue in favor of technologies that maximize exposure. Another source of the dichotomy is the desire of some indie content owners to avoid DRM precisely because of its association with "big media."

The consumer electronics industry's primary incentive, meanwhile, is to design new gadgets to sell to the public quickly. Consumer electronics products have short "half-lives" in the market: they start out with high profit margins, but margins shrink rapidly to virtually nothing as competition destroys uniqueness and newer, cooler products appear on the horizon. CE vendors must constantly refresh their product lines in order to preserve their overall profitability, and refresh cycles tend to get shorter and shorter every year.

For consumer electronics products that handle media content, CE vendors must secure the cooperation of content owners so that brand-name content can be available on the new devices. At the risk of oversimplification¹⁹, the bargain that the two industries have struck has been: we (the media industry) will let you (CE vendors) distribute our content on your products only if we are comfortable that your products won't allow consumers to misuse our content. Therefore you must demonstrate that your products are going to curb misuse to our satisfaction.

This has led to a situation where the CE industry has been given the responsibility for designing DRM systems and thus has taken the lead – by companies acting on their own (Microsoft), by companies licensing technology from third parties (Apple), or via intra-industry partnerships (DVD), consortia (Marlin), or standards bodies (OMA). The media

¹⁸ Rosenblatt, B. *Paying for DRM*. In: Proceedings of BUMA/IViR Symposium: Copyright and the Music Industry: Digital Dilemmas, Amsterdam, Netherlands, July 2003; available at:

<http://www.ivirbumaconference.org/docs/thefutureofdigitalrightsmanagementformusic1.doc>

¹⁹ For example, this argument does not take into account the instances where the media industry is actively interested in reaching a new market enabled by new consumer electronics technology; however, such cases are in the minority.

industry has declined to share in the cost of such systems²⁰ and has only recently started participating in their design in any meaningful way.

As a result, DRM schemes tend to be designed with low cost of implementation as a primary consideration. This has been especially true of the CSS encryption built into DVDs (designed by Matsushita and Toshiba) and Apple's FairPlay. The law that makes hacking DRM illegal, the DMCA²¹, bolsters this situation by deflecting liability for weak DRM from the technology vendor to the hacker²².

In other words, CE vendors generally view DRM as a necessary evil to get content licenses. In most other respects, DRM is antithetical to their business: it costs them money to implement, yet it limits their products' functionality²³.

CE vendors' focus on costs – based on an assumption that their products should all become low-cost blockbusters, like the ubiquitous \$50 DVD player – leads them to favor DRM schemes that have minimal functionality, both with respect to their security strength and their inclusion of consumer-friendly features.

An admitted exception to this is the AACS (Advanced Access Content System) and BD+ DRM schemes for Blu-ray high-definition optical discs, which are far more sophisticated than the CSS scheme for DVDs with respect to both security strength and features for consumers (such as “managed copy”). Two major content owners, Warner Bros. and Disney, have even contributed to AACS's design.

Yet even this is an exception that proves the rule. CE vendors invented these high-def formats to enable them to sell high-margin players to consumers instead of those \$50 DVD players. They feared that both consumers and movie studios would need further motivation to support the new disc formats, so they felt compelled to introduce features that appealed to both parties. Furthermore, there have been disputes over implementation of certain content protection features in players for the new formats²⁴.

Currently, the CE industry sees the Digital Home as its next great opportunity to sell new products to consumers. Unfortunately, “digital home” is a far more complex and ambiguous paradigm than previous CE paradigms such as “portable media player” or even “home theater.” The value propositions – the reasons why consumers should buy equipment and services for home digital media networking – are still relatively unclear. That is one reason why Apple's approach has been more cautious and focused than those of the other axes of power described above: Apple can be said to be waiting for compelling value propositions to emerge before it fully embraces the digital home.

²⁰ On the contrary, the money has flowed in the opposite direction in a couple of instances. For example, some CE vendors pay to license DRM patents from ContentGuard, a firm that is part-owned by Time Warner.

²¹ 17 USC 1201, known informally as “DMCA” because it was included in the Digital Millennium Copyright Act of 1998. There are equivalent anticircumvention laws in other countries, such as those occasioned by the European Union Copyright Directive of 2001.

²² Federal district court judge Lewis Kaplan in *Universal v. Reimerdes* (2000) affirmed that the law should apply regardless of the strength or weakness of the protection technology. See http://w2.eff.org/IP/Video/MPAA_DVD_cases/20000817_ny_opinion.pdf, p. 34.

²³ Clashes between Consumer Electronics Association CEO Gary Shapiro and media industry trade associations have become more frequent and public in recent years. See for example: CEA: RIAA refuses to cooperate, carries out “thinly veiled attack” on fair use. *Ars Technica*, August 10, 2006, <http://arstechnica.com/news.ars/post/20060810-7472.html>. Or, @ MidemNet: MPAA, RIAA, CEA Execs Clash Over DRM & Hardware Controls. *PaidContent.org*, January 20, 2007, <http://www.paidcontent.org/entry/midemnet-mpaa-riaa-cea-execs-clash-over-drm-hardware-controls/>.

²⁴ Hollywood and CE Makers Stall on HD Protection. *DRM Watch*, May 25, 2006, <http://www.drmwatch.com/standards/article.php/3609096>.

Many CE products for the home networking paradigm have been introduced and then quickly abandoned. The current market uncertainty leads to excess fragmentation among the axes of power. Cost of DRM implementation will certainly play a part in determining which axis, if any, ends up as the dominant one when the relevant technologies converge.

The third participant in the DRM tug-of-war is consumers. The AACs example above is evidence of indirect influence that consumers have had on the design of DRM schemes in digital media. Yet it must be said that consumers have had no direct influence, no seat at the table when DRMs are designed. Consumers may enjoy new content business models, but while consumer acceptance of DRM is slowly increasing, consumers still generally dislike DRM²⁵.

Thus, consumers' most effective influence on DRM design is through market forces. Advocacy groups that purport to represent consumer interests, such as the Electronic Frontier Foundation (EFF) and Public Knowledge, have influenced DRM-related legislation and litigation, but their influence on market forces has been strictly limited as well²⁶.

Some scholars²⁷ have pointed to consumers' lack of a seat at the DRM table as *prima facie* evidence of a copyright system that has been effectively hijacked by industry interests, in this case media and electronics. Yet market forces can be powerful, especially when bolstered – as in this case – by the easy availability of content through illegal means.

For example, the major music companies recently decided to eliminate DRM from most paid permanent Internet music downloads – first for Amazon.com, Wal-Mart and other retailers, in order to create viable competitors to Apple's iTunes; then eventually for iTunes itself²⁸. The ultimate objective is to get users to pay for copyrighted works, and the design or absence of DRM thus affects that outcome.

Precious little unbiased analysis has been done on the effects of digital rights technologies on the large-scale economics of the media and electronics industries. Therefore it is premature to say how consumers' merely indirect influence on DRM and related issues influences the balance of economic interests in the copyright system. Only time will tell.

²⁵ See for example the survey results in the In-Stat report *Digital Rights Management Update*, July 2007, <http://www.instat.com/Abstract.asp?ID=212&SKU=IN0703584CM>.

²⁶ One exception to this is the EFF's successful efforts to eliminate the use of copy protection technologies for audio CDs in the United States. In late 2005, a Microsoft Windows internals expert found that one of the three CD copy protection technologies used by the major music companies introduced so-called "rootkit" security vulnerabilities into users' PCs. The EFF capitalized on the ensuing public outcry by inducing a series of events that led to the withdrawal of all three technologies from the U.S. market.

²⁷ See for example: Litman, Jessica, *Digital Copyright*. Amherst, NY: Prometheus Books, 2001. Or, Gillespie, Tarleton, *Wired Shut: Copyright and the Shape of Digital Culture*. Cambridge, MA: MIT Press, 2007.

²⁸ In exchange for variable pricing on iTunes tracks.

About the Author

Bill Rosenblatt, president of GiantSteps Media Technology Strategies, is a recognized authority on digital media technologies, including digital rights management, content management, cross-media strategy, and content production systems, as well as on issues related to intellectual property in the online world.

Before founding GiantSteps in 2000, Bill was a business development executive at a leading technology vendor, an IT executive at major publishing companies, and chief technology officer of an e-learning startup. Bill is the author of several books, including *Digital Rights Management: Business and Technology* (John Wiley & Sons, 2001), and he is editor of the blog Copyright and Technology (<http://copyrightandtechnology.com>).

About GiantSteps Media Technology Strategies



GiantSteps Media Technology Strategies is a management consultancy focused on the content industries that help its clients achieve growth through market intelligence and expertise in business strategy and technology architecture. GiantSteps' clients have included branded content providers, digital media technology vendors ranging from early-stage startups to Global 500 firms, and technology public policy entities in the United States and Europe.