Dealing With Piracy

Intellectual Asset Management In Music And Software

Jeroen van Wijk

ERIM REPORT SERIES *RESEARCH IN MANAGEMENT*	
ERIM Report Series reference number	ERS-2002-86-ORG
Publication	September 2002
Number of pages	18
Email address corresponding author	jwijk@fbk.eur.nl
Address	Erasmus Research Institute of Management (ERIM) Rotterdam School of Management / Faculteit Bedrijfskunde Erasmus Universiteit Rotterdam P.O.Box 1738 3000 DR Rotterdam, The Netherlands Phone: +31 10 408 1182 Fax: +31 10 408 9640 Email: info@erim.eur.nl Internet: www.erim.eur.nl

Bibliographic data and classifications of all the ERIM reports are also available on the ERIM website:
www.erim.eur.nl

ERASMUS RESEARCH INSTITUTE OF MANAGEMENT

REPORT SERIES

RESEARCH IN MANAGEMENT

BIBLIOGRAPHIC DATA AND CLASSIFICATIONS		
Abstract	The music and software industry are employing copy-protection devices in CDs and digital downloads to strengthen their weak appropriability regimes that leave ample opportunities for modern-day piracy. The effectiveness of the strategy is explained on the grounds that (a) the knowledge involved in copy protection is generally too sophisticated for consumers to circumvent, and (b) consumers are not allowed to use circumvention techniques created by knowledgeable third parties. Copy protection is controversial, because it deprives consumers from making home copies of music and software, and hence overrules copyright law that exempts the copying for private use. It is argued that the technical enforcement of copyright protection in the home domain of millions of individuals necessitates a wide consensus between business and society about the legitimacy of private and fair use.	
Library of Congress Classification (LCC)	5001-6182	Business
	5546-5548.6 5548.7-5548.85	Office Organization and Management Industrial Psychology
	HV 8061	Property Protection against Theft
Journal of Economic Literature (JEL)	M	Business Administration and Business Economics
	M 10 L 2	Business Administration: general Firm Objectives, Organization and Behaviour
	K 11	Property law
European Business Schools Library Group (EBSLG)	85 A	Business General
	100B 240 B	Organization Theory (general) Information Systems Management
	3 M	Product Ownership
Gemeenschappelijke Onderwerpsontsluiting (GOO)		
Classification GOO	85.00	Bedrijfskunde, Organisatiekunde: algemeen
	85.05 85.08	Management organisatie: algemeen Organisatiesociologie, organisatiepsychologie
	86.33	Intellectueel eigendom
Keywords GOO	Bedrijfskunde / Bedrijfseconomie	
	Organisatieleer, informatietechnologie, prestatiebeoordeling	
	Recht van de intellectuele eigendom, ongeoorloofde kopieën, beveiliging, gebruiksrecht	
Free keywords	Appropriability, codification, intellectual assets, fair use, digital rights management	

Dealing with piracy
Intellectual Asset Management in music and software

Jeroen van Wijk (jwijk@fbk.eur.nl)

July 2002

Summary
The music and software industry are employing copy-protection devices in CDs and digital downloads to strengthen their weak appropriability regimes that leave ample opportunities for modern-day piracy. The effectiveness of the strategy is explained on the grounds that (a) the knowledge involved in copy protection is generally too sophisticated for consumers to circumvent, and (b) consumers are not allowed to use circumvention techniques created by knowledgeable third parties. Copy protection is controversial, because it deprives consumers from making home copies of music and software, and hence overrules copyright law that exempts the copying for private use. It is argued that the technical enforcement of copyright protection in the home domain of millions of individuals necessitates a wide consensus between business and society about the legitimacy of private and fair use.

Keywords: Appropriability, codification, intellectual assets, fair use, digital rights management

The magnitude of piracy

More than US$ 14 billion is reportedly lost due to worldwide piracy in software and music in 2001. The losses claimed by the music industry amount to US$ 4.3 billion; the software industry claims US$ 10 billion (IFPI 2002; BSA 2002). These figures primarily refer to large-scale counterfeiting operations by organized crime groups, which exploit entire factories to press pirate CDs, but increasingly also involve “garage piracy” that makes use of towers of CD burners in small-scale locations. Estimations of Internet piracy are highly speculative. The music industry assumes that 99% of the music files on-line available in 2001 was unauthorized.

Several questions can be asked about the accuracy of these figures. For example, it is unlikely that each illegal copy displaces a sale at the market price. Many people who download a free copy, or buy at a pirate price, would not buy the same product at a legal market price. Another issue is that losses are calculated on the basis of the estimated reduction in gross revenues rather than in net loss and hence may be significantly overestimated. Disputed is also the contention that free downloading and copying is only bad for music sales. Some musicians experience a significant positive effect from online file sharing[1], and market research has shown that 80 per cent of music down-loaders report their CD purchasing either has remained the same or increased (Ipsos Reid 2002). Nonetheless, the music and software industries have become increasingly concerned with piracy, and have developed a defensive approach to digital distribution. The information technology (IT) industry even complains that there is no compelling content on the internet to drive the adoption of broadband technology and so stimulate demand for their hardware. If music and video were commercially available on the internet in an easy to use format, it would stimulate broadband usage and force consumers to upgrade their computers (Abrahams and Harding 2002).

Piracy involves the unauthorized replication of copyrighted intellectual assets for commercial purposes. Although posing a significant problem for key industries, piracy has received little attention in the literature on intellectual asset management. This is remarkable. The recognition of knowledge as a strategic resource for the firm has aroused a great interest in the value of intellectual assets. The business literature stresses the vital importance of protecting these assets legally, as intellectual property, in order to realize their value (Berman et al 2002; Davis and Harrison 2001; Edvinsson and Sullivan 1996; Glazier 2000; Petrash 1996; Pike 2001; Rivette and Kline 2000; Williams and Bukowitz 2001). The main theme in the literature is the potential benefit of protecting knowledge and information with copyright and trademarks, and, particularly, with patents. It lines out intellectual

asset strategies for the "new battlefields of the knowledge economy" where patents are the "smart bombs of tomorrow's business wars" (Rivette and Kline 2000: xi). The publications excitedly advice managers how to turn intellectual assets into profit centres, but are silent about how to manage piracy.

This article analyses the efforts of the software and music industry to combat home copying and file sharing by copy-protection techniques. The first sections provide a theoretical explanation for copy protection, which is conceived as a knowledge-based strategy that deliberately employs highly codified knowledge to strengthen weak appropriability regimes. Then, the impact of copy protection on relations with other industry sectors and with consumers is discussed. Finally, questions are raised about how firms should manage stakeholder relations when their strategy to protect intellectual assets overrules traditional consumer rights to make home copies.

Reinforcing weak appropriability regimes

A concept that is helpful in analysing the piracy phenomenon is the "appropriability regime", introduced by Teece (1986). The concept of appropriability regime helps to understand the limitations for companies to appropriate their innovations. It is determined by two factors: (a) the efficacy of intellectual property rights' legislation, and (b) the opportunities for third parties to replicate the information (table 1). A regime is "tight" when an innovator is protected by strong patents or copyright, and when replication of the product is not feasible because access to the relevant information is blocked by trade secrets. The appropriability regime is "weak" when the protection conferred by the patents or copyright is limited, and when the information or the product in which it is embedded is easily imitated. Music and software have weak appropriability regimes. It is easy to copy digital music and software, the provisions in copyright law that deal with private copying are confusing and controversial, and the enforcement of copyright in private homes and on the Internet is problematic.

Table 1. Appropriability regimes

		Inherent replicability	
		Easy	Hard
Intellectual property rights	Loose	Weak	Moderate
	Tight	Moderate	Strong

Source: Teece 1986 and 1998

The question is whether firms are passively subjected to their weak appropriability regimes. The term *regime* suggests that the opportunities for appropriation are largely determined by factors external to the individual firm. Both the legal protection opportunities as well as the "inherent replicability" (Teece 1998) of the information involved seem to constitute a given and static environment. In reality, however, firms proactively attempt to increase the efficacy of the regime, either together or alone. They do so in two ways. Firms induce governments and judges to adjust intellectual property legislation, and firms raise the barriers to replication.

The legal dimension of the appropriability regime continuously evolves through case law, by the enactment of new legislation, or by the conclusion of international agreements. These adjustments are largely a response to the changing requirements of industry. For example, until the 1980s, software code used to be only protectable under copyright law. Due to several limitations of copyright, among others that it does not protect against reverse engineering, the software industry elicited further jurisprudence resulting in software becoming also protectable under patent law in many countries. New copyright laws that explicitly address the protection of digital information have also been

adopted in the USA and - via international agreements concluded in the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO) -, in many other countries. These agreements have provided major opportunities for international industry associations to shape the legal dimension of their respective appropriability regimes in the world.

The technical dimension of the regime is also strongly modelled by industry. For example, the copy-protection techniques that are at issue in this article make replication of CDs and digital downloads by consumers troublesome if not impossible. But influencing the 'replicability' of technology is not solely dependent on the skills of the firm to raise technical barriers. It also requires anticipation of the replication capacity of potential imitators. Large or science-based companies possess sophisticated knowledge that enables them to reverse-engineer all knowledge that is embedded in products sold by their rivals and to use that knowledge to create a near imitation. Raising the replication barriers for these actors may be difficult. The barriers that may not keep rivals at bay, may nevertheless deter individuals who have less replication capacity. Apart from differences in technical capacity, the consequences of different forms of replication may differ, as do the causes and objectives of replication. All this variation is important to be taken into account when firms design strategies to reinforce their appropriability regimes.

The codification dilemma

An examination of the factors that determine replication requires a discussion of different forms of knowledge. Of particular interest is the process of knowledge codification, which refers to the transformation of knowledge from a tacit into an explicit form. Tacit knowledge is closely linked to the personal skills and experiences of individuals, while explicit knowledge is disconnected from individuals. Explicit knowledge is formal and systematic, and expressed in words, numbers, scientific procedures, or universal principles (Cohendet et al 2001: 1568) so that it can be stored on a medium.

The interest in knowledge codification is motivated by two main advantages for the firm. Firstly, codification confers knowledge the characteristics of a commodity. In an explicit or formal form, knowledge can precisely be described and specified in terms of content and intellectual properties that reduce uncertainty and information asymmetry in transactions. In addition, codified knowledge is transferable independently from its creator, and can be sold or bought (Cowan and Foray 1997). An important implication is that the ownership of knowledge is transferred from individual employees to the firm's management (Edvinsson and Sullivan 1996; Hall 1993; Ruth and Bukowitz 2001: 101-102). Knowledge may be stored as a database, a software programme, as a new plant variety, or as a patent. The bottom line is that in the stored format, knowledge becomes an asset that is owned by the company and put on the balance sheet. It remains with the company "when the employees leave". Codification may therefore also be a management's tactic to reduce power of skilled employees, or to replace them by semi-skilled personnel who can do the job by following instructions on checklists (Carter and Scarbrough 2000). The second advantage of codification is that it facilitates knowledge diffusion. Tacit knowledge is difficult to transfer. It requires person-to-person contacts, is more time consuming, and more expensive. Codified knowledge, in contrast, enables a quick and cheap diffusion of knowledge within the firm or network. Stored in databases it can be accessed by anyone in the company even at different locations, and facilitates the introduction of new employees (Cowan and Foray 1997: 596-597; Hansen et al 1999: 108-110; Teece 1998: 63).

Knowledge codification also entails disadvantages. If easy replicated within the company, knowledge may also be replicated outside the company's boundaries. Databases or check lists, for example, may be accessed without authorization by competitors. Employees may take away codified knowledge when they move to another firm, despite specific stipulations in their contracts. Patents raise a similar dilemma. Public disclosure of the invention is a condition for patent protection, which makes the invention consequently vulnerable to near imitation by rivals. Knowledge that is codified and embodied into a marketable product facilitates imitation. The opportunities for imitation increase when mass markets are served. Because the product is aimed at a large number of users, it has to be

standardized, which means that all knowledge or art embodied in the product is fully codified. Information and communication technology have greatly facilitated opportunities for both codification and imitation, which induced some authors to speak of the "digital dilemma" (National Research Council 2000). This dilemma is not typical for digitized knowledge, but also applies to knowledge that is codified in other models and languages. For example, in agriculture the knowledge of plant geneticists and plant breeders is codified in the genetic code of new plant varieties. However, varieties are in principle easily copied by farmers who make use of plants' natural feature to reproduce themselves. When codification *as such* facilitates diffusion of knowledge that is both beneficial and detrimental to the company, it is better to speak of *codification dilemma*.

Diffusion requires absorption

The concept of codification dilemma is based on two classic assumptions in economics: (a) that the cost of transmitting information is very low, and (b) that the creator of information has no means to exclude others from using the information he has created (Arrow 1962). Theses assumptions still legitimate the existence of patent and copyright law, but they are not entirely correct. The availability of codified knowledge may be a necessary, but not a sufficient condition for imitation.

Knowledge diffusion is a social process, involving not only transmitters but also receivers of information. Receivers are those actors who have the capacity to absorb, i.e. to understand and employ the information. The process of encoding tacit knowledge must therefore recognize and anticipate the capabilities of targeted receivers. Such anticipation takes place in three inter-related phases that Cowan and Foray (1997: 604) distinguish in the codification process:

* *The creation of messages*: expressing pre-existing knowledge that can be processed as information;
* *The creation of models*: the reorganization (different modelling) of knowledge in order to transform it into information;
* *Language development*: developing a language infrastructure that suits the specific knowledge, such as music, mathematics, expert systems, and novels.

During the codification process, transmitters of knowledge have to encode their messages in the models and language that is understood in the receiving network or community. Receivers, in turn, must be capable to read the language and, to a certain extent, also the model underlying it. However, learning 'the code' of codified knowledge (i.e. its language and model), and building up capabilities to absorb and imitate that knowledge requires time and resources (Cohendet et al. 2001: 1573-1576; Saviotti 1998: 848; Teece 1998: 65). One factor that influences the absorption capability of receivers is the life cycle of the technology. The group of actors that is able to build up capabilities grows as the technology matures. In technological evolution, the emergence of a dominant design heralds the beginning of the paradigmatic phase (Teece 1986: 287). This is a relatively stable period in which knowledge is standardized and codified. In this phase, an increasing number of people learn to imitate or modify the dominant design (Cowan and Foray 1997: 595; Saviotti 1998).

Insight in the phases of the codification process enables us to challenge the classic assumption concerning the very low cost of information transmission. Codified knowledge is not automatically diffused, but depends on the absorption capability of receivers. Given the skewed distribution of time and resources over any population, capabilities to understand and imitate codified information are not equally distributed. Yet, the number of actors that is able to understand 'the code' grows when technology matures. In the context of digital piracy these conclusions imply that we can expect different levels of knowledge of 'the code' of relevant information among (potential) imitators of music and software. Potential imitators consequently differ in their capability to replicate. A distinction can be made between 'inner circle imitators' and 'outer circle imitators' (Table 2).

Inner circle imitators possess the knowledge of the language and the underlying model that is required to reverse-engineer a product, to imitate the product, or to circumvent or decode any protective device that the innovative firm has installed to impede imitation. They all know 'the code'. Inner circle

imitators encompass engineers from rival firms, university scientists, public sector professionals, students, technicians for whom hacking and imitation is a hobby, and engineers employed by criminal organizations who want to seize a share of the market. They do normally not form a community, because of contrasting interests, objectives, and values. Nevertheless, coalitions may arise among some of them when they can benefit from imitation in the outer circle.
Outer circle imitators include individual consumers who imitate a product for private purposes, including non-commercial exchange of imitations among family, friends, and "netizens". They do not have advanced knowledge about the technology involved, but they may acquire specialized devices that do the job for them. Such equipment becomes available as the technology matures and companies begin producing standardized products for mass markets. The devices embody sophisticated, codified knowledge that, in itself, need not to be understood to get them running. Outer circle imitators know 'the code' to start devices that can read the language and model of the codified information and hence facilitate imitation. Examples of such devices vary from standard copy-paste buttons in web browsers and PC operating systems, to CD burners, and the specialized software that enables circumvention of copy-protection devices. Outer circle imitators do not form a community either, but they share an interest in maintaining freedom to make private copies, or exchange copies over the Internet. Their 'natural allies' within the inner circle are the information technology (IT) and consumer electronics companies because they make decoding devices available.

Table 2. Two circles of imitators

	Inner circle imitators	**Outer circle imitators**
Type of actors	Rival companies, criminal organizations, professionals, knowledgeable individuals	Individual consumers
Number of actors	Limited number and identifiable	Millions of individuals spread over the globe
Imitation interest	- Rival firms: reverse engineering to improve own process R&D - Criminal organizations: seizing share of a profitable market - Professionals: improving personal knowledge and status - Hackers: fun, status or political goal	Making copies for private use, more and new music available at low price
Scope copyright law	Commercial imitation forbidden	Imitation for private use exempted Definition of private use differs per country and is not clear
Enforcement copyright	Infringement is - in principle- traceable	Infringement hardly traceable
Effectiveness copy-protection	Low; technical device easily decoded	High; technical device works as 'speed bump'
Legal support copy-protection	Research on, and diffusion of decoding knowledge forbidden	Use of decoding knowledge forbidden

Apart from their skills and purposes, both groups of imitators differ in size. Inner circle imitators are relatively small in number and in principle traceable when they start distributing imitations on the market. It is this group of imitators that is usually focused at in intellectual asset management literature. Outer circle imitators, however, include millions of individuals across the globe. Their copying acts can hardly be traced, and their possible violation of intellectual property rights cannot be determined. Efforts to reduce imitation by outer circle imitators focus therefore on technical barriers, i.e. on raising the level of knowledge required for imitation.

Raising the barriers to replication

Attempts to impede replication directly challenge the assumption of neoclassical economists as that the creator of information has no means to exclude others from using that information. When the diffusion of codified information also depends on the absorption capability of receivers, creators of information have a chance to solve the codification dilemma. They could increase control over the use that third parties make from their information by reducing the chances that the information is absorbed by outer circle imitators. At least four approaches can be distinguished.

1. Firms could make knowledge of the product-related 'code' irrelevant for imitation. They offer their codified product in a package, mixed with "complementary assets", such as marketing, competitive manufacturing, or after-sales support (Teece 1986). Uniqueness of the package mix, or the inclusion of highly competitive assets makes the complete package difficult to imitate, and improves the firm's conditions for appropriation.

2. Firms could generate and use highly specialized codes consisting of technical or local jargon that can only be understood by a select group of actors, and create obstacles to imitation (Cowan and Foray 1997: 599; Cohendet et al. 2001: 1568). In this case, codification has two objectives: to share the knowledge among a certain group (firms, scientists), and to keep others out.

3. Firms could invest more in knowledge creation to "push the frontier of knowledge as fast as possible" (Saviotti 1998: 850). This approach aims to reduce the number of actors that know 'the code' by exploiting lead-time advantage. As it is likely that new, advanced knowledge is more tacit and the number of actors who have access to it limited, this strategy diminishes opportunities for imitation.

4. Firms could block the access to the codified and standardized product with a secretive key. In this approach the number of actors that know the product-specific 'code' is irrelevant. By including an additional piece of encoded knowledge in the product that can only be decoded by a select group of the company's employees, imitation of the product is impossible for as long as the key remains a secret.

All four approaches intend to solve the codification dilemma and so strengthen the appropriability regime. They may be used separately but usually in combination with each other. The first approach is almost always employed. Since software and music is more than just millions of bits, companies have various opportunities to offer unique packages that stimulate the purchase of legal copies. Software consumers require readable manuals to get the programmes running, and favour reliable after-sales services. Music fans often prefer a CD with original cover and booklet that informs about the musicians and lyrics. These complementary assets are vulnerable, however. Counterfeiters imitate the music as well as the printed documentation in a way that is very similar to the original. Moreover, CD covers and booklets are favoured items for shoplifters (Doorduyn 2002). The latter three approaches form the basis of copy-protection techniques.

Copy protection as "speed bump"

The key problem of digital intellectual assets is that they can be replicated without change of properties. Digital information may be copied across media - from hard discs to various formats floppy discs or tape -, or may be sent across networks without any serious loss of quality. The copies are identical to their original source. This situation contrasts with the past in which content could only be distributed as analogue work that was attached to a physical medium, a printed book, or tape. Copies could be made within and across media, but not without a loss of properties. Unique to the digital world is that "content is liberated" from its physical medium (National Research Council 2000: 32-33). Moreover, particularly in the entertainment sector the liberation of content has increased the demand for home copying. Copies are wanted either for time-shifting purposes - recording a television

programme to watch it later -, or for space-shifting purposes - reading, viewing or listening to the protected work through other devices, such as computers, DVD players, game consoles like PlayStation, MP3 players, high-end stereo equipment, and car CD players.

Copy-protection techniques limit the freedom of consumers to make copies of digital information. They intend to contain the 'liberated' content again, and make access to content subjected to control of the copyright holder. Digital Rights Management (DRM) involves a rights model for access to Web-based content. DRM creates various levels of permission for different recipients and controls. It regulates for example who is authorized to use, view or listen to the protected work; how often it can be viewed or listened to; from which computer; and how many copies can be made. Copyright holders use a wide variety of techniques intended to regain control over their content. The most often used techniques are shortly explained in Exhibit 1.

Exhibit 1 Copy-protection techniques

Encryption The information or content is encrypted to transmit it in this form to the receiver. Only the receiver has the key to decrypt the information. Newer systems make sure that the protected file appears in decrypted form only on-screen and never in the random access memory, where computers look into when it is trying to print or copy. This approach blocks copy opportunities during transmission and at the receiving PC.

Distortion Digital distortion is inserted into the sound files of music CDs. It is not audible as long as the CD is played in an audio player, but degrades the sound when the tracks are copied into a digital format and played from a PC's hard drive.

Anchoring The content or information is 'anchored' to a specific programme, user or machine. When anchored to a programme, the document or sound can only be viewed or listened to by using a specific browser plug-in, which is not capable of copying, writing to the disk, printing etc. Examples are Adobe's eBook Reader and Microsoft's Windows Media. More effective control is achieved when the content is anchored to an identifiable user or PC, which are authorized to decrypt the information. Special decoding hardware with a unique identifier may also be installed in the PC.

Trusted systems These involve comprehensive end-to end systems that offer information security and hence facilitate transparency between users and also control digital intellectual property. The main example of a trusted system is the decoder in pay-per-view television. It requires a new design of operation systems, and massive collaboration among software and hardware industries to make such systems operational in computers.

Digital watermarks Encoded ownership information is added to the protected work, visible or invisible. Aim of digital watermarks is not preventing copying, but deterrence, monitoring and collecting evidence for possible infringement. Digital watermarking works in combination with "Web crawlers", special software programmes that systematically search the Internet for documents with a relevant watermark. Machine code for software cannot be watermarked, because the alterations to the code might let computers crash.

Spoofing This is the latest tactic of the music industry to attack the peer-to-peer music networks. The record companies deluge popular P2P music services with thousands of decoy music files that look identical to a sought-after song, but are filled with long minutes of silence or 30-second loops of a song's chorus.

Sources: National Research Council 2000: 157-167; Roush 2002.

The common denominator of the different protection techniques is that they strategically use highly specialized, codified knowledge to raise the barriers to imitation. The protection 'code' is too advanced for most outer circle imitators to be circumvented. Specialized codes, jargon, latest innovations and trade secrets are used to exclude outer circle imitators from access. The level of sophistication of the protection techniques may vary greatly, but for outer circle imitators they all make imitation so cumbersome that buying legal copies is an attractive alternative. Experts therefore believe that copy-protection systems work as a "speed-bump", by frustrating copy efforts of large numbers of individual consumers (O'Connell 2002).

The knowledge-based approach to impede imitation is also vulnerable. It suffers from inner-outer circle collaboration in circumventing protection, and from the absence of industry-wide standards for copy protection. Inner-outer circle collaboration is problematic for copyright holders because inner circle knowledge is transferred and diffused into the outer circle where it is used to break copy protection. Hackers, professionals, academic researchers, advanced students, and other knowledgeable individuals, have the capacity to design and distribute circumventing devices. This knowledge sharing between the inner and outer circle obstructs the knowledge-based approach to reducing imitation. An obvious example of recent inner-outer circle collaboration is the CD burner that replicates CDs which once were thought to be copy-proof. But there are more examples.

In October 2001, the code of Microsoft's DRM was cracked by an anonymous hacker. He placed a circumvention programme on the Internet, according to the attached letter, with the explicit intention to facilitate home copying. The software of the hacker allows someone who purchases a CD with Windows Media files on it to strip off the protections and distribute the files online (Borland 2001). Another example concerns the Content Scrambling System (CSS), a copy-protection device of DVDs. In November 1999, the CSS encryption scheme was broken, when two programmers found out that one manufacturer had not encrypted the decryption key in the software of its DVD player. Examination of the software enabled them to break the protection of that particular player, and provided them insight into the encryption keys used by other players (National Research Council 2000: 172). A free, Windows-based protection circumventing utility, called DeCSS, became subsequently available on the Internet. The third example of inner-outer collaboration involves the copy-protected CDs that Sony began to sell, late 2001. Within a few months Internet newsgroups spread the message that Sony's copy protection could be circumvented by simply scribbling around the rim of a CD with a felt tip marker (Reuters 2002).

To solve this weak aspect of copy protection, the software and entertainment industry resorted to the government. Legislation was designed to thwart further inner-outer circle collaboration in cracking copy protection. The USA was the first country that outlawed the design of measures that circumvent copy-protection techniques. The Digital Millennium Copyright Act (DMCA), adopted in 1998, includes two regulations for this purpose: The *access-control provision*, which prohibits the circumvention of technical protection measures used by copyright holders to control access to their works, and the *anti-device provisions*, which bans devices that are designed or produced primarily for purposes of circumventing technical protection measures. DMCA-like legislation was subsequently also introduced in many other countries that adhere to the WIPO Copyright Treaty (WCT). In the European Union, anti-circumvention has become forbidden with the adoption of the European Union Copyright Directive (EUCD), which must be implemented in the member states by the end of 2002.

The second weak point in copy protection is the absence of an industry-wide consensus on a technology standard. Attempts to achieve such a standard have foundered so far. The main example is the Secure Digital Music Initiative (SDMI) that started in 1998 to find an effective response to music piracy. Around 200 companies from the recording and technology industries worked together to secure digital songs, but failed to produce commercial results. The boom of file-sharing applications, such as Napster and KaZaA, overtook the companies involved, while none of the copy-control systems SDMI released survived the hackers who were invited to crack the code. The main problem in the SDMI was, however, the opposing interests of the industries involved. The *entertainment industry* covers the copyright holders. They aim at effective DRM systems that make unauthorized copying virtually

impossible, and have a common interest in blocking imitation by consumers. The *Information Technology (IT) industry* has an interest in selling PCs to consumers. And consumers demand PCs on which music playback is possible and which can be used to store other copyright-protected works. Some observers speak of a divide between 'Hollywood' and 'Silicon Valley'. The IT industry would perceive protection of copyrights primarily the business of the entertainment industry, which should respond to the present imitation challenges with a different business model. The entertainment industry replies that there is no business model that enables competition when the products are elsewhere available for free (Harmon 2002). The third sector is the *consumer electronics industry* that has a specific interest in home copying because they sell DVD recorders, MP3 players, and CD players. The prime interest of consumer electronics industry is that copy-protection techniques and DRM systems are compatible with the various types of hardware. This requires a widely accepted technology standard.

The failure of the industry to reach consensus over a copy protection and DRM standard has resulted in demands for government intervention. Much to the satisfaction of the American entertainment industry, US senator Hollings, in March 2002, introduced a bill that would require manufacturers of devices ranging from PCs to VCRs to implement copy protection in their devices. The bill is bitterly opposed by the technology industry (Abrahams and Harding 2002). The European Commission so far has confined itself by urging the industry to come up with a solution quickly.

In the absence of a standard, various companies have begun experimenting with copy-protection. By the end of 2001, the five major record companies set up two separate DRM-based subscription services for music: *Pressplay*, which offers songs from Sony, EMI and Universal, and *MusicNet* offering artists from the labels of EMI, Warner and BMG. These services were introduced as legal alternatives for notorious file-sharing services like Morpheus, KaZaA and Grokster. Both Pressplay and MusicNet are highly cumbersome for consumers. The music offered with both services is limited to what is offered by their own labels, the music is incompatible with existing software, and is expensive ($2 for an individual song). Pressplay allows customers to burn 10 songs to a CD each month, but only two songs from the same artist. In 2001, the record companies also began selling copy-protected CDs, mainly in Europe. Universal has released 2 million copy-protected CDs in Germany, but kept the technology confined to non-blockbuster albums. Sony Music Europe shipped 11 million copy-protected CDs, including albums from celebrities such as Celine Dion, Jennifer Lopez and Shakira.

Until present, the rate of success in digital protection devices is generally low. Apart from code cracking and other circumvention methods, protected CDs sometimes failed to play on some audio equipment, or made computers crash. BMG has already switched back production to "clean" unprotected CDs, following consumer complaints (Abrahams and Harding 2002).

Opposition to copy protection

The copy-protected CDs and DRM systems have been hailed with criticism. The "stealth CDs", as the protected CDs have been dubbed by opponents, have provoked considerable public opposition. The web pages of American and European civil society organizations, such as the Electronic Frontier Foundation, Home Recording Rights Coalition, DigitalConsumer.org, Eurorights.org, the Free Software Foundation, and the European Consumers' Organization BEUC[2], reflect a broad disapproval of the growing control of copyright holders. None of the organizations opposes copyright protection as such, but they all are concerned about the restrictions to the legal right of consumers to use content that they have legally purchased. They defend the legitimacy of making private copies for time shifting and place shifting purposes to use them on the large variety of audio-visual and computer equipment, from VCR to lap top.

The consumer criticism on copy protection and DRM addresses a highly contentious issue of copyright, namely non-commercial copying for private use. Private use is part of a number of

exemptions under copyright laws. In most countries copyright is limited in that some forms of non-commercial or private use of protected material do not require authorization and the payment of royalties. Usually are exempted the copying for personal use, some copying for scientific purposes - such as quoting -, and some use of protected material in the public interest - such as lending by libraries. In the USA and UK these exceptions are known as “fair use” respectively “fair dealing”. However, the boundaries of what constitutes private or fair use are far from clear and seem to evolve in time.

Economists argue that the rationale for the private use exemption is one of sheer necessity. A normal market for copies of copyrighted work failed to develop, because the transaction costs incurred by enforcing the rights and the sale of copies to individual consumers exceeded the value of the copies. Instead, governmental intervention created a ‘market’ (Towse 2000: 15). In many countries royalty collecting societies were founded that took over the clearance, royalty collection and enforcement from individual right holders. Most European countries and the USA also introduced levies on blank media, such as cassettes and CDs, or on digital devices that can be used for copying. The purpose of the levy system is to collect money to compensate copyright holders for legitimate copies made by individuals. The collected money is distributed back to record companies and broadcasters, estimating the payments by examining record sales and the programme logs of broadcasters.

The emergence of copy-protection techniques and DRM systems challenges both the fair use exemptions as well as government intervention. Following the economists logic, the introduction of DRM and copy protection reduces transaction costs for both enforcing copyrights and the sale of individual copies just to a level that the costs no longer exceed the value of an individual copy. A market could then emerge, making continued government intervention in the music market superfluous. This argument would explain the strong demands to abolish the levy on blank media by the entertainment and the IT industry during a DRM workshop in Europe (European Commission 2002). The levy system is loathed by the entertainment industry because of its “rough justice”, the IT industry opposes levies for reason that it raises the sales price of its products, and consumers organizations are concerned that the co-existence of both the levy and DRM systems makes consumers pay twice.

More controversial, however, remains the issue of private copying. The new technology deprives consumers from their opportunities to make personal copies of protected work. This has given rise to two opposing positions. On the one hand are the copyright holders who hold that this limitation of copyright was borne out of necessity, and that the private use exemption was therefore only temporary. New technologies change the rules of the game. Consumers have to adjust their expectations and behaviour to the new realities, and must pay for using protected work. On the other hand are the consumer and civil society organizations, supported by the IT and consumer electronics industry. They consider the private use exception an affirmative right of consumers. Consumers should retain the freedom to privately use purchased items, as they like.

Due to the controversy about private and fair use, the new copyright laws that have been adopted in the USA and Europe do not establish clear rules. The Digital Millennium Copyright Act is vague whether or not circumvention of protection devices is permitted to enable fair use (NRC 2000: 174, 318), and the EUCD provides a long list of exceptions in view of private use, which are optional for EU member states to include into their national laws.

Closely related to the private use issue is the discussion over the anti-circumvention provisions in the new copyright laws. Many American academics believe the DMCA discourages scientists from publishing in the area of encryption through the fear of legal action inspired by the DMCA (Knight 2002). Opponents refer to recent incidents involving the DMCA. In September 2000, the music industry collaborating in the Secure Digital Management Initiative (SDMI) had posted music samples that carried digital watermarks on its website, and offered $10,000 to anyone who could crack the code. A team of American researchers, led by Edward Felten, professor digital security at Princeton University, took up the challenge and quickly claimed success. He forfeited the prize money to avoid

signing a secrecy agreement, and planned to reveal the methodology at an international conference in Pittsburg. The American Recording Industry then sent Felten an intimidating letter stating that such a presentation could be seen as a violation of anti-circumvention regulations under the DMCA (Fox 2001). The other incident involved the Russian scientist Sklyarov, who went to the United States to present a paper on cryptography. Sklyarov is an employee of Elcom Ltd. and was charged with "trafficking" in software designed to circumvent copy protections in Adobe's eBook Reader software, which is a criminal violation of the DMCA. He was arrested, and only after a huge public furore, was allowed to go home. But the charges against his company were not dropped. Elcome's software could be used to make illegal copies of an ebook protected by Adobe, but it could also be seen as restoring fair use rights that Adobe's programme prevents (Wildstrom 2002).

Implications for Intellectual Asset Management

The key issue in the civil society opposition to copy protection and DRM is that software code has achieved a higher status than legal code, or in the words of Lessig (1999) "code has become law". According to Lessig, software code regulates all aspects of our life, more pervasively than any other regulator. Initially, Internet software code overruled the system of legal protection, and created liberty for consumers. Future code, however, will create architecture of centralized control, if everyone using the Internet is going to be identified, their actions tracked, their actions restricted by code. However, the main problem, says Lessig, is not the regulating impact of software code, but the absence of democratic decision-making. Legal protection requires political decisions that may seek a balance between private and public interests. As it come to technological content protection, it is up to the private company to balance the different interests. Lessig speaks of West Coast code - the software from Silicon Valley - that overrules East Coast code - the legislation from Washington. The impact may be bigger. Considering the worldwide diffusion of American software, the reality is that the American West Coast code supersedes not only America's national laws, but also those of most countries in the world.

The implications for intellectual asset managers are immense. Lawyers are used to legal battles with rival companies and criminal organizations that are behind the large-scale piracy operations. These operations might be complicated, enduring and expensive, but they are also relatively well ordered and the legal departments are equipped to handle them. Knowledge-based protection of intellectual assets changes this situation, because copy protection inherently involves political issues. When technical protection overrules the law, industry claims superiority over the legislator. As a result, civil society demands for democratic decision-making will directly be addressed to the industry, and requires the legal departments to prepare themselves for a battle that is primarily political in character, and involves millions or even billions of individual potential opponents across the globe. These opponents also happen to be customers, and that means the corporate image is at stake. It seems therefore inevitable that knowledge-based protection of intellectual assets is integrated into an interdisciplinary corporate strategy, which avoids a fight with the industry's primary stakeholders, and initiates an open dialogue with civil society on what should be the values and norms with respect to non-commercial copying and file exchange of copyrighted work for private use.

Notes

[1] See the critical article on the music industry's approach of online music by the artist Janis Ian. The article "Risky Business. The Internet Debacle: An Alternative View" was published in the June 2002 issue of the *Performing Songwriter Magazine* and can be downloaded from Ian's homepage: www.janisian.com

[2] See the websites of these organizations: www.eff.org, www.hrrc.org, www.digitalconsumer.org, www.eurorights.org, www.fsf.org, www.beuc.org.

References:

Abrahams, Paul and Harding, James (2002) The digital Divide. *Financial Times*, 21 May.

Arrow, Kenneth J. (1962) Economic Welfare and the Allocation of Resources for Invention. In *The Rate and Direction of Inventive Activity*, ed. R.R. Nelson, pp. 609-626. Princeton University Press, Princeton, USA.

Borland, John (2001) Hacker cracks Microsoft anti-piracy software. *News.com*, October 19. www.news.com.com/2100-1023-274721.html

Berman, Bruce (ed.) (2002) *From Ideas to Assets. Investing wisely in Intellectual Property*. John Wiley & Sons, New York, USA.

Business Software Alliance (BSA) (2002) *Seventh Annual BSA Global Software Piracy Study.* www.bsa.org/sweeps/2002_piracyStudy.pdf

Carter, Chris and Scarbrough, Harry (2000) *Regimes of knowledge, Stories of power: A treatise on Knowledge Management*. Discussion Paper, University of Leicester, Management Centre, UK.

Cohendet, Patrick and Meyer-Krahmer, Frieder (2001) The theoretical and policy implications of knowledge codification. *Research Policy*, **30**, 1563-1591.

Cowan, Robin and Foray, Dominique (1997) The Economics of Codification and the Diffusion of Knowledge. *Industrial and Corporate Change*, **6(**3), 595-622.

Davis, Julie L. and Harrison, Suzanne S. (2001) *Edison in the Boardroom. How leading companies realize value from their Intellectual assets*. John Wiley & Sons Inc, New York (USA) and Toronto (Canada).

Doorduyn, Yvonne (2002) 'Bauer raakt nooit meer op'. *De Volkskrant*, 20 June.

Edvinsson, Leif and Sullivan, Pattrick (1996) Developing a Model for Managing Intellectual Capital. *European Management Journa*l, **14**(4), 356-364.

European Commission (2002) *Digital Rights Management (DRM) Workshop*. Organised by the European Commission's Information Society Directorate General, Brussels, 28th February 2002. www.europa.eu.int/information_society/topics/multi/digital_rights/events/index_en.htm

Fox, Barry (2001) Disharmony. *NewScientist.com*, 7 June. www.newscientist.com

Glazier, Stephen C. (2000) *Patent Strategies for Business.* Third Edition. Law & Business Institute, Washington, D.C., USA.

Hall, Richard (1993) A framework linking intangible resources and capabilities to sustainable competitive advantage. *Strategic Management Journal*, **14**, 607-618.

Harmon, Amy (2002) Piracy, or Innovation? Its Hollywood vs. High Tech. *The New York Times on the Web*. March 14. www.nytimes.com

International Federation of the Phonographic Industry (IFPI) (2002) *Music Piracy Report 2002*. www.ifpi.org/site-content/library/piracy2002.pdf

Ipsos Reid (2002) Fee-Based Online Music Faces Uphill Battle. Press Release 25 February. Ipsos Reid, USA. www.ipsos-reid.com

Hansen, Morten T., Nohria, Nitin and Tierney, Thomas (1999) What's Your Strategy for Managing Knowledge? *Harvard Business Review*, **77**(2) 106-116.

Knight, Will (2002) Controversial copyright clause abandoned. *NewScientist.com news service*, 15 April. www.newscientist.com.

Lessig, Lawrence (1999) *Code and Other Laws of Cyberspace*. Basic Books, New York, USA.

National Research Council (NRC) (2000) *The Digital Dilemma. Intellectual Property in the Information Age.* Committee on Intellectual Property Rights and the Emerging Information Infrastructure of the Computer Science and Telecommunications Board. National Academy Press, Washington D.C., USA.

O'Connell, Patricia (2002) A Speed Bump vs. Music Copying. *Business Week Online*, January 9, 2002. www.businessweek.com/bwdaily/dnflash/jan2002/nf2002019_7170.htm

Petrash, Gordon (1996) Dow's Journey to a Knowledge Value Management Culture. *European Management Journal*, **14**(4) August, 365-373.

Pike, Christopher G. (2001) *Virtual Monopoly*. Nicholas Brealey Publishing, London, UK.

Reuters (2002) Cheap pen cracks 'copy-proof' CD. *ZDNet UK News*, May 25. www.news.zdnet.co.uk.

Rivette, Kevin G. and Kline, David (2000) *Rembrandts in the Attic. Unlocking the Hidden Value of Patents*. Harvard Business School Press, Boston, USA.

Roush, Wade (2002) The Death of Digital Rights Management? *Technology Review*, **105**(2), 24-25.

Teece, David (1986) Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy* **15**, 285-305.

Teece, David J. (1998) Capturing Value from Knowledge Assets: The New Economy, Markets for Know-How, and Intangible Assets. *California Management Review*, **40**(3), 55-79.

Towse, Ruth (2000) *Creativity, Incentive an reward. An Economic Analysis of Copyright and Culture in the Information Age*. PhD thesis, Erasmus University Rotterdam, the Netherlands.

Wildstrom, Stephen H. (2002) "Fair Use" Is getting Unfair Treatment. *Business Week Online*, May 14. www.businesweek.com.

Williams, Ruth, L. and Bukowitz, Wendi R. (2001) The yin and yang of intellectual capital management. The impact of ownership on realizing value from intellectual capital. *Journal of Intellectual Capital*, **2**(2), 96-108.

Publications in the ERIM Report Series Research* in Management

ERIM Research Program: "Organizing for Performance"

2002

Trust and Formal Control in Interorganizational Relationships
Rosalinde Klein Woolthuis, Bas Hillebrand & Bart Nooteboom
ERS-2002-13-ORG

Entrepreneurship in China: institutions, organisational idendity and survival. Empirical results from two provinces.
Barbara Krug & Hans Hendrischke
ERS-2002-14-ORG

Managing Interactions between Technological and Stylistic Innovation in the Media Industries. Insights from the Introduction of eBook Technology in the Publishing Industry
Tanja S. Schweizer
ERS-2002-16-ORG

Investment Appraisal Process in the Banking & Finance Industry
Mehari Mekonnen Akalu & Rodney Turner
ERS-2002-17-ORG

A Balanced Theory of Sourcing, Collaboration and Networks
Bart Nooteboom
ERS-2002-24-ORG

Governance and Competence: How can they be combined?
Bart Nooteboom
ERS-2002-25-ORG

ISO 9000 series certification over time: What have we learnt?
Ton van der Wiele & Alan Brown
ERS-2002-30-ORG

Measures of Pleasures: Cross-Cultural Studies and the European Integration
Slawomir Magala
ERS-2002-32-ORG

Adding Shareholders Value through Project Performance Measurement, Monitoring & Control: A critical review
Mehari Mekonnen Akalu & Rodney Turner
ERS-2002-38-ORG

Web based organizing and the management of human resources
Jaap Paauwe, Rolf Visser & Roger Williams
ERS-2002-39-ORG

---

* A complete overview of the ERIM Report Series Research in Management: http://www.ers.erim.eur.nl

ERIM Research Programs:
LIS Business Processes, Logistics and Information Systems
ORG Organizing for Performance
MKT Marketing
F&A Finance and Accounting
STR Strategy and Entrepreneurship

Challenging (Strategic) Human Resource Management Theory: Integration of Resource-based Approaches and New Institutionalism
Jaap Paauwe & Paul Boselie
ERS-2002-40-ORG

Human Resource Management, Institutionalisation and Organisational Performance: a Comparison of Hospitals, Hotels and Local Government
Paul Boselie, Jaap Paauwe & Ray Richardson
ERS-2002-41-ORG

The added value of corporate brands: when do organizational associations affect product evaluations?
Guido Berens, Cees B.M. van Riel & Gerrit H. van Bruggen
ERS-2002-43-ORG

High Performance Work Systems: "Research on Research" and the Stability of Factors over Time
Paul Boselie & Ton van der Wiele
ERS-2002-44-ORG

Diversification and Corporate Governance
George W. Hendrikse & Aswin A..C..J. Van Oijen
ERS-2002-48-ORG

Governance Structure, Product Diversification, and Performance
Aswin A. Van Oijen & George W. Hendrikse
ERS-2002-51-ORG

Global Sourcing: Fad or Fact?
Michael J. Mol, Rob J.M. van Tulder, Paul R. Beije
ERS-2002-55-ORG

Internationalization Of Management Buyouts: Firm Strategies And Venture Capitalist Contribution
Mike Wright, Andy Lockett, Paul Westhead, Hans Bruining
ERS-2002-58-ORG

The Importance Of Customer Satisfaction In Organisational Transformation: A Case Of A Dutch Temporary Employment Agency
Martijn Hesselink, Ton van der Wiele and Paul Boselie
ERS-2002-60-ORG

A Study On The Applicability Of SERVQUAL Dimensions For Web Sites
Jos van Iwaarden, Ton van der Wiele
ERS-2002-61-ORG

Entrepreneurial Orientation In Management Buy-Outs And The Contribution Of Venture Capital
Hans Bruining and Mike Wright
ERS-2002-67-ORG

The odd role of proximity in knowledge relations - High-tech in The Netherlands
Gerben van der Panne, Wilfred Dolfsma
ERS-2002-75-ORG

Organizing as Improvisations (Methodological Temptations of Social Constructivism)
S. Magala
ERS-2002-76-ORG

Best Practice in Company Standardisation
Florens J.C. Slob, Henk J. de Vries
ERS-2002-81-ORG

Standardisation education
Henk J. de Vries
ERS-2002-82-ORG