Vural Ünlü

Content Protection

Economic Analysis and Techno-legal Implementation

Herbert Utz Verlag · München

Law and Economics

Herausgegeben von

Prof. Dr. Jörg Finsinger, Universität Wien
Prof. Dr. Michael Lehmann, Universität München
Prof. Dr. Arnold Picot, Universität München

Band 29

Zugl.: Diss., München, Univ., 2004

Bibliografische Information Der Deutschen Bibliothek:
Die Deutsche Bibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über
http://dnb.ddb.de abrufbar.

ISBN 3-8316-0462-2

Printed in Germany

Herbert Utz Verlag GmbH, München
089-277791-00 · www.utzverlag.de

Overview of contents

Table of contents

1 Introduction

1.1 Scope of the problem

In today's information society, the commercialisation of creative works and the industries associated with this field have assumed a significant role with regard to the economy and employment [Wirt01,14-17]. It is estimated that currently 5% to 7% of the Gross Domestic Product is generated in branches of the economy concerned with the creation or commercialisation of copyrighted products [Krög02,14]. Such industries are currently threatened by extensive product piracy. Representative bodies of the entertainment industry claim that the negative impacts on these industries are significant. For example, the International Federation of the Phonographic Industry (IFPI) estimates in their *Commercial Piracy Report 2004* that commercial piracy of physical formats accounted for an estimated US$4.5 billion in 2003 in terms of illegal sales worldwide [IFPI04]. The Motion Picture Association of America (MPAA) estimates that the US motion picture industry alone loses $3 billion in revenues yearly [MPAA04]. Neither of these statistics includes losses due to Internet piracy, which are assumed to be substantial.

However, the scope of losses claimed by the media industries should be accepted with caution. A careful study of the assumptions upon which the calculations of losses are based suggests that the figures have been obtained simply by multiplying the estimated number of pirated media products by the retail price. Thus, these theoretical calculations are based on the assumption that in a world without piracy, the present consumers of pirated products would instead purchase legitimate content. However, without price reductions, it is unlikely that all illegal users would purchase the legitimate products, in the event that piracy was prevented by whatever means. It can therefore be seen that the methodology employed in some studies of illegal commercial copying leads to exaggerated estimates of losses in revenue [CSTB00,188-190].

Furthermore, the point should be made that not all media segments are equally affected by piracy. This is because not all media segments are dependent on the generation of direct revenues. Media companies can also derive indirect revenue from advertising, which is based on the generation of attention [ScHe02,38-45]. As Figure 1.1/1 illustrates, the ratio between direct and indirect revenues differs according to the media segment. Whereas a book publishing company generates almost its entire turnover by means

2 Foundations

2.1 Terminology

Economists, lawyers and security engineers have differing viewpoints and use their own terminology within their own fields of research, generally with little consensus concerning the meaning of key terms. Therefore, an important starting point for interdisciplinary research is the clear definition and consistent use of terms. Three terms which exhibit a high degree of semantic divergence are: "media good", "property" and "optimal level of protection". These terms will be discussed below.

Various researchers have provided definitions of the term "**information good**" (also referred to as a "**media good**" or "**cultural product**"). Phetig defines an information good as "a set of information pieces which is well-defined in its contents, its quantity and its specific presentation" [Peth88,463]. In contrast, Shapiro and Varian take a broader view by defining the term "information goods" as anything that can be digitised or encoded as a stream of bits [ShVa99,3]. In fact, the term tends to be defined differently depending on the technical, functional, economic [Dete01,10-14] or legal context. The semantic hierarchy adopted for a media good is based on Anding's definition [Andi04,18-23] and is illustrated in Figure 2.1/1. Thus, "characters" (i.e. digits, letters, etc.) are defined as the fundamental units of a semantic library. A set of characters that are syntactically interrelated is referred to as "data", e.g. words or numbers. Only when data can be interpreted by the recipient do they assume meaning and hence become "information" [MBKP04,55]. Information can therefore be considered to be a message created by a sender that can be contextually understood by a receiver. Information can be regarded as a good in an economic sense if it (i) provides utility to at least one consumer, (e.g. by enhancing knowledge or providing entertainment), (ii) enjoys market demand, and (iii) is scarce, i.e. not readily available [Kief01,141-142]. Information that fulfils these three criteria will be referred to as "content". If the content is a copyrighted Original Work of Authorship (OWA), it can become a piece of "Intellectual Property" when certain conditions set by legislators are met (see Section 2.3.2). It is important to note that technical protection can be applied to any digital (e.g. binary) representation of a media product, regardless of whether or not it is protected by law [Bech02,16]. This is the reason why the generic term "content protection" is used in this thesis in preference to the expression "copyright protection".

Technicians are primarily interested in the first three levels, in other words the representation of media goods in binary form. Economists focus their interest on the content level, viewing contents as goods that can be traded in a marketplace. Finally, legal scholars are concerned with the interpretation and formulation of statutes concerning works defined as media goods endowed with property rights.

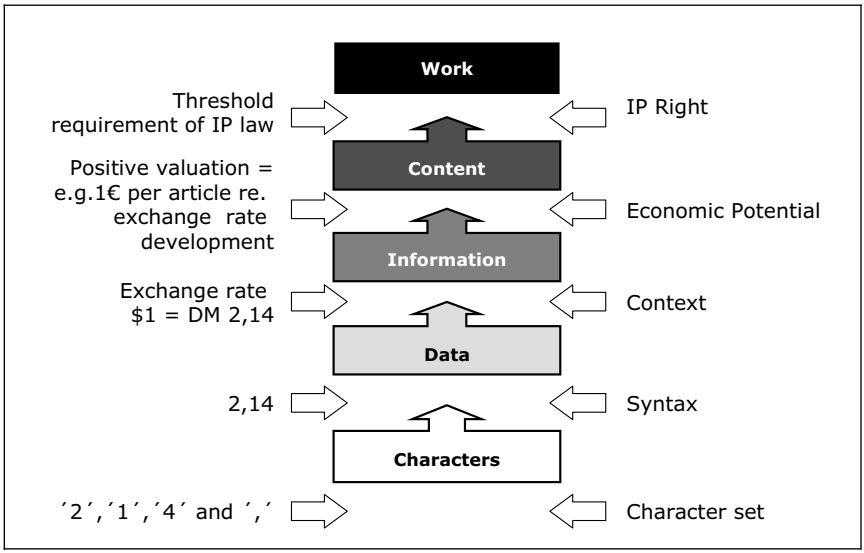

Figure 2.1/1: Media products: From character to intellectual property

The concept of "**media companies**" also requires clarification. Schumann and Hess define twelve types of media company, based on three segments of the value chain (production, bundling and distribution) and four types of mass media (print, broadcasting, storage media and online media). This is illustrated in Figure 2.1/2 [ScHe02,9]. A narrower view is taken by Albarran and Chan-Olmsted, who see media companies as institutions engaged in the production and dissemination of media products targeted to consumers [AlCO98,4]. According to this view, inputs are usually unrefined pieces of raw content (such as scripts, music video clips and videotapes) provided by original creators of works (including reporters, editors, producers), and outputs are bundled products such as magazines, music records or TV programs. Therefore, media companies that act at this (second) level of the value chain usually are not the legal creators of intellectual property, but acquire licenses to exploit the economic value of media products. In this

thesis, media companies will be referred to henceforth as "content providers".

The concept of "**property**" is also understood differently by economists and lawyers. Property is of pivotal importance in the fields of both law and economics. While the economic notion of property is relatively straightforward, encompassing all rights of individuals with regard to the use of valuable resources [Alch65,817], there is no universally accepted legal definition of the term, although it is used prominently in many doctrines and statutes. Some legal scholars consider property rights as a "bundle" of exclusive rights [Penn90]. Although most legal definitions of property also include rights pertaining to exclusive use and alienability, this is not an exhaustive list of valuable rights. Thus the economic notion of property is more far-reaching than the legal use of the term. The differences between legal and economic notions of property are due to the fact that the definitions serve different purposes. Legal definitions are intended to differentiate property from other legal areas, an objective referred to by Penner as "individuation" [Penn97,32]. In contrast, the economic concept is mainly concerned with the role of exclusive rights to scarce resources in promoting the efficient allocation of those resources. Because of the significant differences between legal and economic notions of property, some economists prefer to use the term "entitlements" rather than "property rights" [MeSm01,380].

Furthermore, due to differing objectives and notions of efficiency, the concept of an **"optimal" level of copyright protection** exhibits semantic variation depending upon whether an economic, technical or public policy perspective is used. From a public policy perspective, an optimal level of protection is achieved when socially optimal levels of investment and consumption regarding creative materials are established through statutory means. In contrast, technical and economic viewpoints relate to technical rather than legal property rights. Therefore, it is difficult to compare the technical and economic notion of optimal copyright protection with that of the public policy perspective. There is also a substantial difference between the technical and economic optima. From a technical perspective, the optimal technical level of copyright protection would be considered to be achieved (i) when the protection is *unconditionally secure*, i.e. it cannot be breached even with infinite computational resources, or (ii) when it is *computationally infeasible* to crack the technical security mechanism, i.e. the cost of breaching the security exceeds the value of the attacked information, or the time required exceeds the useful

lifespan of the information. In contrast, from an economic viewpoint, the optimal level of technical copyright protection would be that where certain economic objectives, such as profitability targets, are maximised. A technically optimal level of protection may be higher than an economically optimal level, since protection costs tend to increase significantly with the overall protection level. Although toleration of a lower level of protection might make a successful piracy attack more likely, it could optimise overall profitability.

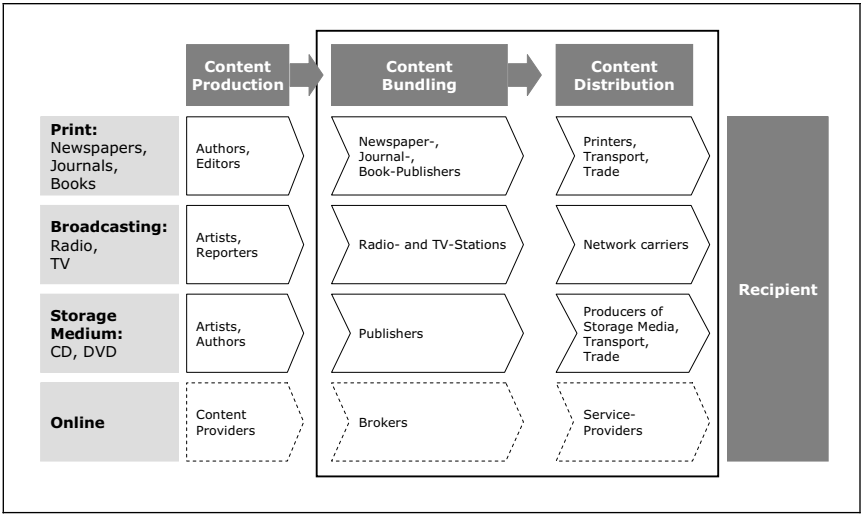

Figure 2.1/2: Types of media companies [ScHe02,10]

In the field of security engineering, an "**attacker**" (also referred to as an "*adversary*" or "*opponent*") is defined as someone who aims to overcome a security mechanism, regardless of whether the motivation is honourable (e.g. vulnerability testing during product development) or malicious. In this context, the computing community differentiates between "*hackers*" (or "*white hats*"), who have honourable motives, and "*crackers*" (or "*black hats*"), who have malicious intentions [MavO03,6-7]. Unauthorised reproduction and distribution of analogue or digital content is often referred to as "*piracy*". Pirates can use a variety of channels for distributing illegal content, including physical distribution (e.g. hard goods piracy involving video CDs) and electronic distribution via the Internet. Although online piracy is widespread, using Peer-to-Peer (P2P) networks, File Transfer Protocol (FTP) sites, Internet Relay Chat (IRC) channels and auction sites, it cannot be quantified. "*Copyright infringement*" is defined as the unauthorised use of copyrighted work in a form that violates one of the copyright owner's exclusive

rights, such as the right to reproduce the work or to make derivative works that are based upon it [Litm01,19].

"**Security**" is generally defined as freedom from attack or as the condition of safety. Figure 2.1/3 illustrates how the basic elements of security terminology relate to one another.

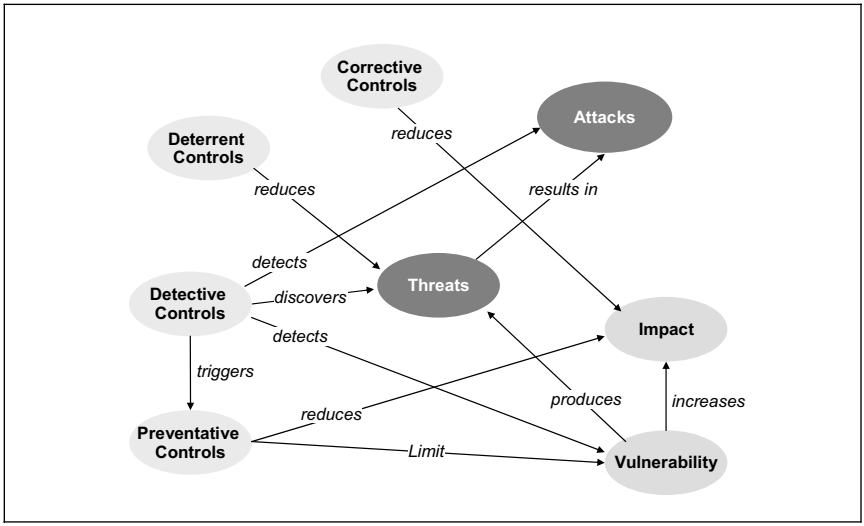

Figure 2.1/3: Types of information security controls [TiKr00]

A "**threat**" is a potential cause of an unwanted event, which may result in harm to an institution. Threats may originate from internal or external sources and may be caused by deliberate or accidental action [MavO03,2]. A "**vulnerability**" (or "weakness") is a characteristic of an information system which can be exploited by an attacker. "**Controls**" are countermeasures for vulnerabilities, and can be physical, technical or administrative. There are four types of control [TiKr00]: preventative, deterrent, corrective and detective. *Preventative controls* aim to prevent the occurrence of attack or to render an attack unsuccessful or reduce its impact by restricting the free use of computing resources and the operations accessible to users. *Deterrent controls* reduce the probability of an attack by discouraging users from intentionally breaking information security policies. Such controls are usually based on threats of negative consequences, which are intended to influence a potential attacker to not violate security (e.g. threats ranging from embarrassment to harsh punishment). It can be argued that deterrence is a form of prevention, because it may prevent a potential attacker from acting. *Corrective controls* reduce the impact of an attack by restoring pre-

attack conditions. *Detective controls* identify attacks after they have occurred and trigger preventative or corrective measures. Thus, when all aspects of security control are implemented, there is a greater likelihood of preventing and/or stopping attacks.

2.2 Stakeholder analysis

As stated at the end of Section 1.2, this dissertation focuses on the interests of content providers and shows how they can be assisted by techno-legal means. However, content providers do not operate in a vacuum, and are dependent upon other stakeholders in order to realise their aims. These stakeholders have diverging objectives and a certain influence with regard to the future application of protection measures, whether technical or statutory. These stakeholders must be identified and their objectives and degree of influence assessed in order to analyse whether the interests of the content providers can be realised, what opposition and potential alliances are to be expected and which interests should be taken into consideration when implementing protection measures. Stakeholder Analysis (SA) constitutes a valuable methodology in this respect [WaMa02,1-23]. Stakeholder analyses of DRM have been carried out by the New Millennium Research Council [NMRC03] and by Fetscherin [Fets04]. However, it is difficult to compare the results, since each study identifies a different set of relevant stakeholders.

As the first step in undertaking a stakeholder analysis, eight main groups of stakeholders are distinguished that have a legitimate interest in the subject of content protection (see Figure 2.2/1): IP creators, the content industry, collecting agencies, the telecommunications industry, the consumer electronics (CE) industry, consumers, civil liberties groups (CLGs) and legislators. More homogeneous stakeholders can be identified, such as schools, libraries and the research community, however, they can be neglected at this point [CSTB00,61-75].

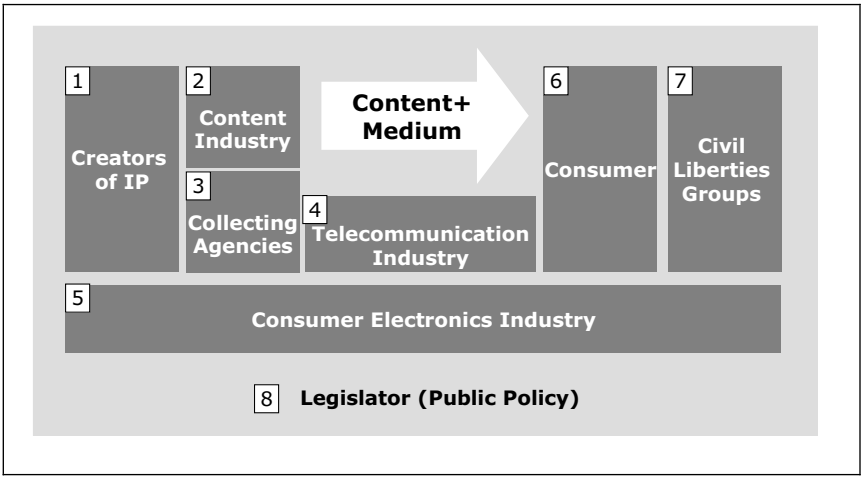

Figure 2.2/1: Overview of stakeholders in the digital rights management domain

In line with SA methodology, first the interest of these stakeholders in techno-legal protection measures will be discussed and then their power of influencing the achievement of their goals will be assessed. Influencing power can be determined in terms of economic resources, level of concentration and organisational efficiency. The analysis that follows is based on expert opinion reflected in the literature.

Creators of IP, the original creators of content (e.g. artists, painters, writers, etc.), are interested in the protection of their work, which is their primary source of income. However, they are also interested in the free flow of information as a basis for their inspiration and knowledge, in order to create new content. On their own, they tend to be poorly organised, and do not negotiate usage terms vis-à-vis the consumer [Fets04]. Their interests are mainly channelled through artists guilds, content industry and collecting agencies.

Copyright industry organisations are trade associations that represent content owners and bundlers, for example, the IFPI, the Recording Industry Association of America (RIAA) and major music labels. These organisations advocate statutory and technical protection to protect the economic interests of their members [Mitc04,3]. They are opposed to fair use laws and advocate anti-circumvention legislation [NMRC03,5-6]. Due to their concentration, the significant monetary contributions of their members, and their professional organisation, they represent the core pressure group of

producers and bundlers of media goods [Fets04].

Collecting agencies are usually non-government organisations that administer the rights of copyright holders [Meye01,13-17]. They manage the process of enforcement on behalf of creators, thus providing a transaction cost-effective mechanism for applying billing rights. They represent the interests of many IP creators, and are therefore negatively affected by digital piracy and have an interest in the protection of Intellectual Property. However, DRM poses a threat to collecting agencies, since the transaction cost rationale on which their existence is based is diminished in the light of the cost-efficient rights management techniques of a DRMS [Mösc99,169].

The telecommunications industry electronically distributes digital content, both legal and illegal, to end consumers such as Internet Service Providers (ISPs) and cable operators. A significant part of the billable traffic is attributable to acts of piracy, particularly in the case of P2P traffic [Musi04,6]. However, telcos are starting to move out of the commodity-like access business, extending their business model by offering legal content [Wirt99,19-22]. Thus, they are also becoming interested in ways to provide and enforce content protection. Due to their extensive economic resources and relatively high level of concentration, they are considered to be an influential stakeholder [ZPSA99,62-65].

The consumer electronics (CE) industry produces software- and hardware-based end-consumer devices for digital media consumption (e.g. computers, DVD players and mobile handsets). One the one hand this industry wants to produce equipment that is accepted by end consumers, with few technical restrictions and a high degree of usability. On the other hand, it is necessary to provide high security levels in order to motivate the content industry to supply digital products for the end-user devices [NMRC03,5]. The interest of the CE industry is to promote market-driven solutions rather than solutions mandated by public policy. Like the content industry, the CE industry has a substantial economic size, is well-organised and well-funded [Wirt01,16;Musi04,5].

Consumers of digital content include end consumers, businesses, schools, research institutions, etc. Most piracy is carried out by end consumers who illegally consume unprotected media goods. Loosely speaking, consumers oppose technical usage restrictions and favour fair use legislation [Slow03;Cost01]. Economically, they are very powerful, but they are too atomised to have a noticeable influence [Krem01]. However, they pursue their interests by electing politicians and by means of civil liberties groups.

Civil liberties groups (CLGs), such as NetCoalition, Electronic Frontier Foundation and the Electronic Privacy Information Centre, represent the interests of end consumers by protecting their online civil liberties. They oppose the enforcement of copyright legislation, advocate the free flow of information and favour the extension of the fair use doctrine. First and foremost, they are opposed to technology solutions that limit user rights [NMRC03,9]. They are very active at the political level and are regarded as the counterpart of the content industry.

Legislators determine the legal environment that is binding for all stakeholders. Their objective is to maximise social welfare. Legislators are affected by piracy in the short-term only to a small degree, possibly though a reduction of tax income and a loss of jobs in the affected media industries. Legislators are influenced by the lobbyism of economically strong pressure groups [Fets04].

Based on this analysis, the stakeholders can be mapped according to their stance toward DRM and their power to influence content protection mechanisms. This is illustrated in the power grid shown in Figure 2.2/2. In this figure, different shades are used to indicate the position of the various stakeholders in the value chain, in terms of production, distribution and consumption.

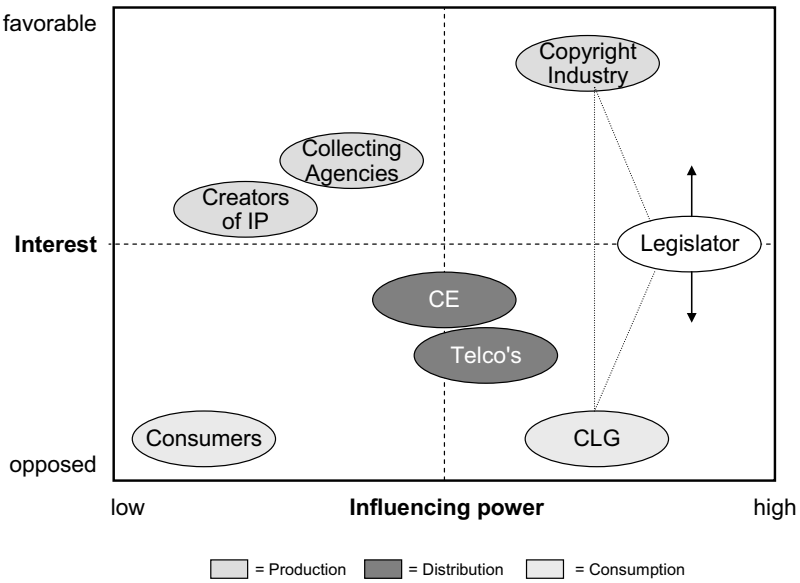

Figure 2.2/2: Stakeholder power grid

This power grid helps to identify the stakeholders that determine the technical development and legal environment relating to content protection. From the right-hand side of the grid it can be seen that the content industry faces opposition to strong content protection from three influential pressure groups: the Consumer Electronics Industry, the Telecommunications Industry and Civil Liberties Groups. Furthermore, the interest of the most influential stakeholder, the legislators, is considered to be more or less neutral. Therefore, these results suggest that the conflict regarding Intellectual Property protection technologies and legislative changes will be fought out between these players. The most important constellation is the "power triangle", where both the content industry and civil liberties groups are trying to influence legislators to enact legislation favourable to their interests.

Stakeholder analysis is undoubtedly a useful tool for assessing the power structure within a market. However, the stakeholder matrix is based on individual expert opinion, which may be biased. Such analyses are therefore not necessarily a true reflection of reality. Further study is required in order to reach a complete understanding of the goal conflicts and balance of power among the different stakeholders. However, this analysis provides a good basis for

3 Techno-legal perspective

The purpose of this chapter is to analyse the technical structure of currently existing DRMSs and to show how to implement a desired level of content protection using technical means. To this end, first the security requirements of multimedia applications will be presented, together with a threat model. The model determines the goals of the pirates as well as addressing some general strategies of media companies for protecting themselves from such threats. Certainly, the analysis of the motivation and situational characteristics of persons who engage in acts of piracy is an important step in the formulation of effective measures to alleviate the problems associated with piracy. In the next step, the technical foundations of a DRMS are introduced through the construction of an idealised reference model. Media managers can use this classification scheme to classify existing DRMS solutions and obtain an overview of the non-transparent market for DRMS solutions. For this purpose, three representative solutions in the DRMS marketplace will first be described; then the functional and technical scope of a DRMS will be inferred. The logical and physical architecture of a DRMS are presented in Section 3.2.2. The most important functions of a DRMS are then described in Section 3.2.4, and the core technologies underlying these functions are discussed in Section 3.2.3. Three prominent DRMS solutions are subsequently presented, which are used to illustrate how these functions and techniques are currently implemented in the marketplace. This descriptive part of the dissertation builds on and extends a Wirtschaftsinformatik (information systems) paper published by Hess and Ünlü [HeÜn04] and a conference paper presented at the 15th Biennial Conference of the International Telecommunication Society in Berlin [ÜnHe04].

Following this descriptive analysis, Section 3.3 aims to provide a normative analysis of how a certain protection level can be effectively implemented. This depends upon various critical premises, such as the attacker model and other environmental assumptions that will be defined beforehand. A model will be proposed in which the main determinants of security are logical and physical protection based upon the robustness of access control and the tamper-resistance of the playback device. Various security mechanisms are classified according to their protective strength. Due to the fact that the security engineering environment is similar to a technological arms race between security engineers and attackers, it is essential to have a clear understanding of the motivation and objectives of the attackers and their state-of-the-art

attack instruments and approaches. The chapter concludes with a summary of the results and an indication of emerging requirements which may provide a focus for future discussion.

3.1 Security model

3.1.1 Security objectives and policies

The threat of information piracy represents a significant risk for media companies. Other industry segments are also exposed to information system attacks, which can result in significant financial losses. Recently, Information Technology (IT) systems have become more vulnerable to such threats, due to the increasing ubiquity and interconnectivity of computer networks, making them more interdependent and more accessible to a large number of individuals. **Security**, broadly defined as the protection of desired objects against malicious actions for the purpose of avoiding, detecting and/or recovering from attacks, is therefore becoming a pivotal objective for all types of institution.

In this context, IT systems are used for a variety of applications, increasingly dedicated to multimedia content, such as DRM-related systems. Such systems have their own inherent security requirements for protecting sensitive rights and media assets, for identifying entities in transactions and for providing data integrity. Understanding and specifying security requirements is an essential aspect of establishing effective, interoperable DRMS standards [Schn01,55]. In broad terms, the three fundamental goals of Confidentiality, Integrity and Availability (easily remembered by their initials "CIA") can be discerned [Schn01,55-76]. They will be presented below, together with an introduction to related forms of malicious attack.

Confidentiality refers to limiting information access and disclosure to authorised users, and to preventing access by and disclosure to unauthorised users. Confidentiality should be maintained at all times, i.e. when data are stored, processed and transmitted. Cryptographic techniques, discussed in later sections, can be used to achieve confidentiality.

Integrity refers to the trustworthiness and accuracy of information resources. It must be ensured that information has not been modified inappropriately, whether by accident or deliberately [Selk00,22-24].

Availability refers to the necessity of ensuring that the systems are operating at the required times, i.e. they are accessible to legal users when needed. A well-known type of attack against availability is a denial-of-service attack, where a web server is disabled by an avalanche of requests.

Secure, trustworthy interactions are also essential features of DRMS installations. Based on the above-mentioned global IT security goals, refined DRMS security requirements, in conjunction with concrete security measures, are described by Dittmann [Ditt00,11] as follows.

Content confidentiality measures protect content from disclosure to unauthorised entities (e.g. by means of encryption techniques).

Content integrity measures verify that the content has not been altered. The manipulation of data can be detected by means of digital signatures and fragile or robust digital watermarks [Selk00,22-24].

Origin authenticity measures permit authentication of the content origin (also effected by means of digital signatures and fragile or robust digital watermarking techniques) [Selk00,24-25].

Entity authenticity measures enable the communicating entities to verify that the entities are those they claim to be (e.g. via authentication protocols) [BeSW01,2].

Non-repudiation mechanisms provide proof of whether or not a particular event or action has occurred. Digital certificates and protocols are used to establish information accountability. These mechanisms are based on digital signatures combined with the use of certification authorities, time stamping techniques and evidence recording.

Renewability refers to the fact that once a protection measure has been defeated, it should be replaced by a new secure mechanism without rendering the legacy devices useless. This feature is also sometimes referred to as "self-stabilising robustness".

These *security objectives* are quite abstract, and need to be substantiated in a context-specific *security policy* that specifies in a written statement the high-level strategies and procedures [Schn01,297-299]. This ensures that the goals are met by defining which states of the respective system are considered to be safe or unsafe [Bish03]. Such specifications usually determine a set of operations that an application or software component is or is not authorised to perform. Often, a security policy also defines whether

actions involving access to resources (such as input-output devices, data ports, etc.) are permissible or not.

In the context of the media industry, the global aim is to safeguard secure dissemination of the media products and to prevent the illegal consumption of pirated content. More concretely, the system should ensure that pirates cannot obtain an unprotected media product by hacking the security mechanism (e.g. encryption) surrounding the product or by compromising the playback client so as to gain illicit access to protected media products. The following sections discuss the cost-efficient enforcement of security policies by means of *security mechanisms* (e.g. technical tools, methods, algorithms. etc.)

Nevertheless, it should be emphasised that too narrow a focus on security objectives and policies would be short-sighted. In addition to enforcing security, a DRMS can also establish new forms of business model. In order to be consistent with the interests of the stakeholders involved, other critical DRMS requirements must be considered [Sand02], particularly (i) mobility (i.e. attaching rights of use not only to the playback device but also to the individual user), (ii) user-friendliness (and non-intrusiveness), (iii) affordability of the playback device, (iv) interoperability and (v) compatibility with the letter and spirit of codified law and overall societal interests.

3.1.2 Threat model and environment

Although security objectives and policies are an important starting point, they cannot be stipulated independently of the environmental situation. To determine the required security level of a system against possible attacks, it is necessary to define a **threat model** which identifies the threats that a technical installation must counter and analyses the objectives and resources of the adversary [Schn01,279-280]. For instance, the motives, computational power, monetary resources and technical capabilities of an attacker should be analysed, together with various environmental assumptions regarding the data and systems under attack [MavO03,4]. More concretely, the following questions should be answered: What is the motivation and capability of the attacker? What level of attack can be expected? What level of damage is acceptable? Threat models are useful in order to guide software and hardware designers in determining adequate levels of reliability and the security countermeasures required. In other words, it is futile to attempt to develop a secure system without understanding the nature of the threats which pose a need for security [Schn01,279]. Furthermore, in line with the approach taken by this thesis, the scope of security

measures of a media company is dependent on budgetary constraints. In addition, there is a correlation between the level of security and the overall protection costs. Therefore, the use of a threat model can also assist in the design of the most cost-effective anti-piracy measures.

Threat modelling begins with the identification of potential risks faced by a firm, including fraud, malicious acts, pranks, natural disasters, user errors and so on [GAOR98]. Microsoft employs a plausible taxonomy of security threats [Micr00], as shown in figure 3.1/1.

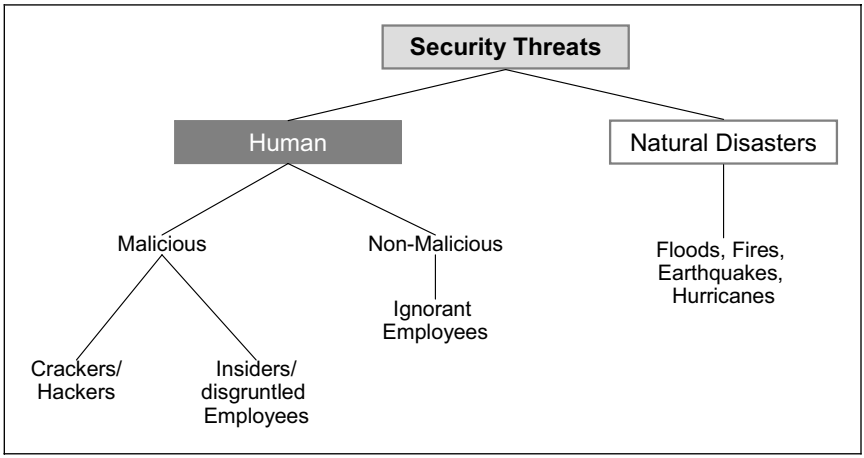

Figure 3.1/1: Security threat classification [Micr00]

The focus of this dissertation is on malicious attacks by outsiders, which can be motivated by personal reasons (e.g. revenge), material gain (e.g. commercial piracy), a wish for publicity (e.g. notoriety and popularity) or other factors. With regard to the media segment in particular, an attacker can harm the economic interest of content providers through various forms of attack [JMVS04,6-7], the most important being "freeing content" and "freeing the application" [MavO03,5].

"**Freeing content**" refers to removing usage restrictions, so that the pirate can consume, distribute or even commercialise an unauthorised copy of a media product.

"**Freeing the application**" is related to deactivating the copy protection scheme of a playback device through tampering techniques. The end goal is to prevent the playback client from executing effective usage control over the protected content. In this case, the attacker either tries to discover the secrets of the code

4 Economic perspective

Based on what has been written so far, it may seem that technological protection measures are a panacea for protecting content. However, it should be kept in mind that complete protection is neither technically feasible nor economically sound. It is true that technological protection measures have the potential to re-privatise media products through the exclusion of free riders. At the same time, such measures lead to higher costs along the whole value chain, possibly resulting in a decline in utility on the consumer side [ÜnHe03]. Depending upon the level of security desired by media companies, a DRMS involves investments for integrating the system into the system environment, for the training of staff and for the alignment of business processes. As a result, the trade-off between the costs and benefits of varying degrees of content protection gives rise to a need to identify an appropriate level of technology-based protection. The associated costs cannot yet be recovered by additional sources of revenue from digital business models, and the potential generation of micropayment revenues faces the problem of prohibitive transaction costs, particularly billing expenses [Schm01,445].

Past approaches to an adequate level of security have focused primarily on technical aspects [Oppl97;Bhim96;Sher00;Finn98], while neglecting the economic dimension. There has been little research in the area of determining the optimal level of information security and the corresponding level of investment. The problem of developing an appropriate, useful approach for choosing the optimal level of investment in multimedia security has yet to be addressed by scientists and practitioners. In the future, this class of investment will constitute an increasing proportion of the total investments made by media enterprises.

In this chapter, the cost-benefit problem will be illuminated by means of three different methods:

In Section 4.1, a simple portfolio-based approach based on media asset value maps is developed in order to assess the optimal level of protection heuristically. This section is based on a contribution for *Information Management* by Ünlü, Rauchfuß, Hess and Faecks [ÜRHF04b]. Although this approach is intuitively understandable, it has major conceptual drawbacks, such as the neglect of cost considerations.

Section 4.2 will address these shortcomings through the consideration of classical finance-based concepts, focusing on Net Present Value (NPV) and Value at Risk (VAR) methods. This

approach attempts to quantify the costs of potential attacks and the probability of their occurrence, balanced against the costs of preventing attacks and operating extra security measures. Based on the monetary relationship between risk and benefit, it is possible to decide whether it is worthwhile to protect content against acts of piracy. However, in determining the optimal level of security, the reliability of decisions based solely on financial concepts is limited, since it is difficult to measure the benefits associated with higher security levels and to quantify the risk in relationship to the security level.

Therefore, in order to address this issue, Section 4.3, which constitutes the major part of this chapter, proposes a game-theoretic model. Rather than focusing on a concrete business context, the model attempts to analyse the economics of a DRMS on a more abstract level. Here, the emphasis is on understanding the structural relationships of the costs and benefits associated with a DRMS. The target function is not a sophisticated measure of the discounted streams of cash flow, but rather a simple profit function with highly idealised assumptions regarding the composition of the margin and cost structure. First the basic model is developed, the equilibria are calculated, and a comparative static analysis is performed to aid in understanding the behaviour of the model. Subsequently, the premises of the basic model are changed, by modifying either the utility function for the consumer or the profit function of the original content provider. A total of three model extensions are presented, to aid in improving the conceptual understanding of the economics of a DRMS.

4.1 Media asset value model

Various factors influence the decision-making process of a media company concerning whether or not and to what extent a media product should be protected using technical protection measures. Based on the approach suggested here, these factors can be roughly divided into two main groups: enterprise-related and customer-related. Each view can be illustrated by means of a **media asset value model**, indicating the positioning of the media products under investigation. As a result, a heuristic evaluation of the level of protection which is economically feasible for a media product can be derived after consolidating two media asset value maps [ÜRHF04b,56-57].

The **customer-related** media asset value map assesses the illicit copying potential on the basis of two influencing factors: the interest of potential customers in the product and their technical access

capabilities. Thus the two dimensions "willingness to copy" and "ability to copy" are scrutinised. A variety of factors can be suggested with regard to the willingness to copy, including the willingness to pay, the degradation level of pirated products (constituting a decrease in utility of the pirated product vis-à-vis the original product), the transaction costs involved in the acquisition of the pirated products (particularly search and download costs), and the availability of substitute products. Factors influencing the ability to copy include the broadband capacities of customers relative to the requirements for copying, and the technical affinity and literacy of the customers. For instance, intuitively, it would seem that popular music songs for a young target group possessing high technical affinity would require more protection than generic text-based content that targets an older, less technically literate consumer group. If the interest in a media product is especially high and the access possibilities are very good, it is worthwhile to use a higher level of protection for the content, because the danger of illegal circulation through pirated copies is relatively high. A product which evokes little interest or which is targeted toward consumers without technical capabilities for unlawful acquisition requires no, or a low level, of DRMS protection.

In contrast, the **enterprise-related** media asset value map assesses the necessity of content protection on the basis of internal company criteria. Again, these can be summarised in terms of two dimensions. The first dimension includes quantitative, measurable financial aspects such as expected turnover or profits which can be achieved by means of the product, excluding any piracy effects. The second dimension involves the *value curve of the content*, in the sense of a media asset life cycle [Dete01,14-15]. The life cycle of a product is thus the number of months or years until no more significant product turnover can be generated. In this media asset value map, the position of products with a long life cycle and a high sales potential (e.g. blockbuster films) indicates that these products require a high level of protection. In contrast, in proportion to the potential losses suffered through pirated copies, equivalent protection costs can be excessive for products with a low sales potential and a short lifespan (e.g. weather news).

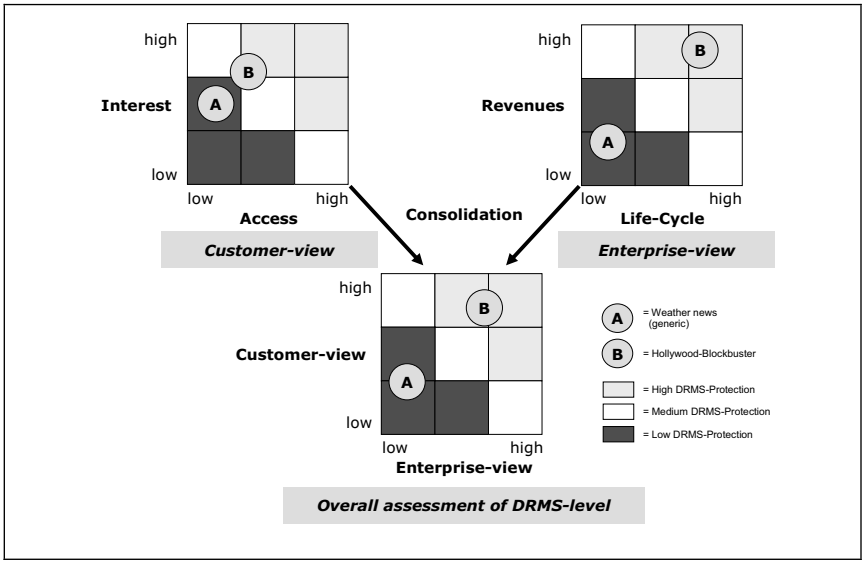

Figure 4.1/1: Media asset value maps for customers and enterprises [ÜRHF04b,57]

The two views can be consolidated in order to arrive at a decision matrix with normative protection recommendations. For this purpose, an individual or uniformly-distributed weighting of the customer and enterprise views can be selected (see Figure 4.1/1). By means of the consolidated map, it is possible to make a simple evaluation of the necessity for a DRMS and the level of protection required, on the basis of the internal and external factors. However, this approach can be considered to be a heuristic method, that therefore does not guarantee an optimal solution. In addition to the often-discussed drawbacks of a portfolio approach, another objection which can be made is that the cost structure of DRM measures is not fully taken into account.

In spite of various model defects, and the fact that it may not lead to an optimal solution, this method nevertheless provides a useful first approach to assessing the cost-benefit factors of a DRMS.

4.2 Classical finance-based approaches

Since the tool presented in Section 4.1 is qualitative in nature and somewhat primitive and not grounded in theory, there is a need to develop a more sophisticated quantitative methodology rooted in existing concepts found in the economic literature.

Classical economic modelling techniques can make a valuable contribution to arriving at optimal decisions regarding DRMS implementations. A sound economic justification of information security investments can be made via formalised cost-benefit concepts such as Net Present Value and Value at Risk. However, choosing the optimal level of security is complex due to the difficulty of measuring (i) the risk and monetary requirements for different levels of security and (ii) the benefits associated with these levels of security. It is therefore necessary to assess how these two components, risk and benefit, can be quantified. The economic rationale is straightforward: If the potential loss due to an act of piracy is small and the risk of occurrence is low, the prevention of this form of attack may not be worth the investment required.

In connection with this more sophisticated approach, it is necessary to refer to the term "risk" as well as some related concepts. **Risk** can be viewed as the likelihood that a threat materialises [TuWM96]. Clearly, risk is unavoidable and a firm must always tolerate some level of risk. In a more detailed definition, risk can be considered as the sum of *threats* (attacks which cause damage), *vulnerabilities* (the susceptibility to threats) and *asset value* (the worth of the threatened assets). The goal of risk management is to identify, quantify and control uncertain attacks, in order to minimise damage and optimise resource allocation for security purposes. Risk analysis is the aspect of risk management that aims to minimise risk by permitting the deployment of protection measures which are in line with the relative threats, vulnerabilities and value of the resources.

Either a quantitative or a qualitative approach can be pursued in the determination of risk exposure. The quantitative approach analyses the monetary costs of risk and risk reduction techniques based on the probability that an attack will occur, the costs of potential damage, and the costs of possible mitigating actions (for instance, through the calculation of the life cycle costs of the security services). When no reliable data concerning the probabilities and costs are available, a qualitative approach can be used that interprets risk in softer terms [StGF02,23]. A combination of quantitative and qualitative methods may also prove useful.

Established security evaluation methods, including *OCTAVE, attack trees* and *Common Criteria* still exhibit major disadvantages. While OCTAVE is concerned with risk assessment for an entire organisation rather than for individual applications, the Common Criteria methodology is considered to be excessively complex and time-consuming. More work remains to be done to develop consistent, reciprocally comparable methodologies for security evaluation [JMVS04,5]. Recent research on multi-attributive risk assessment [BuFi02] and risk-centric decision processes [Feat03] seems particularly promising.

Based on the quantified risk and benefits, it is possible to determine the economic attractiveness of a certain DRMS installation through classical concepts such as Net Present Value and Value at Risk.

The **Net Present Value** (NPV) of a given DRMS installation is calculated by assessing the cash inflows and outflows associated with that installation for each year and then discounting them against the cost of capital. A company will choose the DRMS installation with the highest NPV (see Figure 4.2/1).

A more progressive approach to risk assessment is the **Value at Risk** (VAR) method, which has gained wide acceptance in financial research [Jori97]. When applied in a security context, VAR estimates the maximum potential loss as a result of security breaches during a target time period, with a given level of confidence. In a more formal definition, VAR quantifies the quantile of the projected distribution of losses over a given time horizon [JaRe01,8]. VAR is useful in providing a theoretically-based, numeric measure of information security risk. Based on this risk measure, the best possible trade-off between risk and the cost of providing security services can be determined. The VAR that is calculated by means of the methodology described here is dependent on the particular security installation. It can be seen that different countermeasure solutions will affect the threats and their probability of occurrence, thus influencing the resulting VAR level. Using this methodology, a company will select the security installation which minimises the sum of the VAR and the TCO (see Figure 4.2/1).

5 Public policy perspective

In the IO model, optimal business strategy is determined on the basis of market structure. However, media firms should also take public policy reaction into consideration. A restrictive stance by governments toward DRMS solutions, due to possible negative welfare implications of (strong forms of) content protection, may result in a weakening of certain DRMS protective features. For example, the strength of technological protection is heavily dependent on legal circumvention prohibitions. A relaxation of these and other stipulations could make existing DRMS installations obsolete or could necessitate additional investment to adjust the technological protection level. Such adjustments could be expensive, technologically difficult or even impossible to implement. Thus, government reaction clearly has direct repercussions with regard to the selection of concrete DRMS installations. It is therefore necessary to analyse likely reactions toward DRMS solutions.

This will be done by looking at normative guidance -drawing from previous research of Bechtold [Bech02], Kurth [Kurt02] and Musick [Musi04]- will be offered based on a qualitative law and economics approach, and principles for the formulation of suitable public policy reactions will be discussed.

5.1 Public policy options

To meet the challenges of the digital era, governments have the following options: a laissez-faire approach, compulsory licensing of digital content, and imposition of technical mandates [Musi04]. These alternatives will now be presented and their economic efficiency and fairness examined. This section does not aim to present a comprehensive legal and economic analysis of the copyright regime, but rather is meant to provide a basic overview of the legal options and possible trends, so as to assess the potential implications for media companies in the decision-making process for selecting a DRMS installation.

Other public policy actions are conceivable, such as increasing the penalties for infringers or using publicity campaigns to promote consumer awareness of the legality of Internet use and digital copying. However, these actions cannot be viewed as stand-alone public policy options and therefore will not be analysed in the following sections.

5.1.1 Laissez-faire

One option is for governments to take a libertarian "laissez-faire" approach to DRM, allowing natural market forces to present the most efficient market solution. This approach, favoured by the technology industry and promoters of a free market, allows individual content holders, consumer electronics manufacturers, and developers of security techniques to decide on the most efficient solution.

This hands-off approach could offer some advantages to the media market. In this scenario, market-based solutions would lead to a variety of types of DRMS, and it would be left to consumers to decide which content they want to purchase, with which protection features. With this libertarian approach, DRM decisions are made not by legislators, but by the stakeholders involved, who are the best informed concerning the relevant issues. Furthermore, in a libertarian paradigm, market-based solutions are considered to be the most economically efficient. This approach creates a climate of competition and innovation among stakeholders at the production and distribution levels of the value chain, promoting the best solutions for consumers. New standards and methods of content commercialisation can flourish, undisturbed by government regulations [Kurt02,11-12].

The laissez-faire option builds on the idea that market-based forms of DRM technology will eventually allocate and enforce (technical) property rights for digital content, and that efficiency gains can be realised through the differential pricing capability of DRMS solutions. The role of property rights and the benefits and conditions of price differentiation will therefore be discussed before DRMS efficiency arguments are analysed.

5.1.1.1 Property rights and efficiency implications

Economists justify different forms of property rights as a way of overcoming the public-goods/free-rider obstacle to information production and distribution, so as to promote efficient market transactions that result in information being transferred to its most highly valued use [Lehm83].

Well-defined, well-administered property rights are essential for the smooth functioning of markets and the economic well-being of society [Alle00,898]. They establish ownership of goods and services as well as the recourse that parties have in potential disputes, in order to establish cost-efficient transactions among individuals. The function of boundaries in supporting property rights is often

described by the famous phrase "good fences make good neighbours" from Robert Frost's poem "The Mending Wall" [Fros13].

In the law and economics tradition, property rights are principally viewed as economic instruments for allocating creative resources. From this perspective, the existing copyright regime should not be an absolute, inviolable set of rights to which either content creators or consumers are entitled, but rather a dynamic regime that can be aligned with technical developments in order to meet welfare objectives.

Intellectual property legislation comprises one of the many types of property rights that govern both tangible and intangible property. However, due to the unique features of IP, a different type of regulation is necessary than that usually applied to classical forms of tangible property. It has already been pointed out that the ICT-induced **public goods problem** could lead to an underproduction of media goods. Therefore, legislators need to grant some property rights to prevent media goods from becoming public goods [Lehm83]. However, the granting of such rights could result in a monopoly situation, causing economic inefficiency and leading to a permanent loss of well-being in society.

Often copyright and other property rights are referred to as "**legal monopolies**", as they confer some exclusive rights to their creators. However, this direct link is not justified, as Machlup emphasizes:

> *"From an economic point of view, "property" and "monopoly have almost nothing to do with each other. A seller who owns his wares has property but no monopoly if many other people independently sell similar things in the same market. A seller who can control the price of what he sells, because no one seriously competes with him in the market, has a monopoly but not property if he does not own what he sells" [Mach58,54].*

Machlup points out that the monopoly status resulting from property rights can be somehow diminished through the availability of substitute goods. If substitute products are readily available, then competition will bring down the price down to marginal cost [Boyl00,2018]. The level of substitutability is economically expressed with the notion of *cross-price elasticity*, which indicates how strong the demand for a good A decreases, when the price for the substitute B is lowered [Dete01,15]. In fact, for the case of the cultural industries, the monopoly status can be low of creators for

generic, low-value content (such as threepenny novels); but this is certainly not the case for the bulk of cultural products. Creative products, almost by definition, have unique, distinctive characteristics that appeal to certain consumers. Therefore, most media goods are not as easily interchangeable as other commodities, and the resulting competitive pressures may be lower in other markets [Bech02,291].

It can therefore be stated that property rights grant temporary monopoly rights to the authors of copyrightable works [CoUl88,135]. The standard economic objection to monopolies is that a monopolist, with a given cost structure, will have a lower output and demand higher prices than is the case in a competitive industry. As a result, society is faced with a net loss of allocative and economic efficiency, because prices are driven above marginal costs [ScOt95,74-78]. Consumers who are willing to pay a price which is higher than the efficient marginal cost but lower than the monopoly price are priced out of the market. This detrimental effect of monopoly pricing is quantified by the concept of **deadweight loss** [Vari96,413-415].

The following diagram shows the loss of efficiency resulting from a monopoly. If it is assumed that a competitive firm and a profit-maximising monopolist have the same cost structure, the monopolist will have higher prices and a lower output than the competitive firm. The monopolist price for an information good is set above marginal cost which leads to a deadweight loss and therefore a loss of static economic efficiency [DaWh67,360].

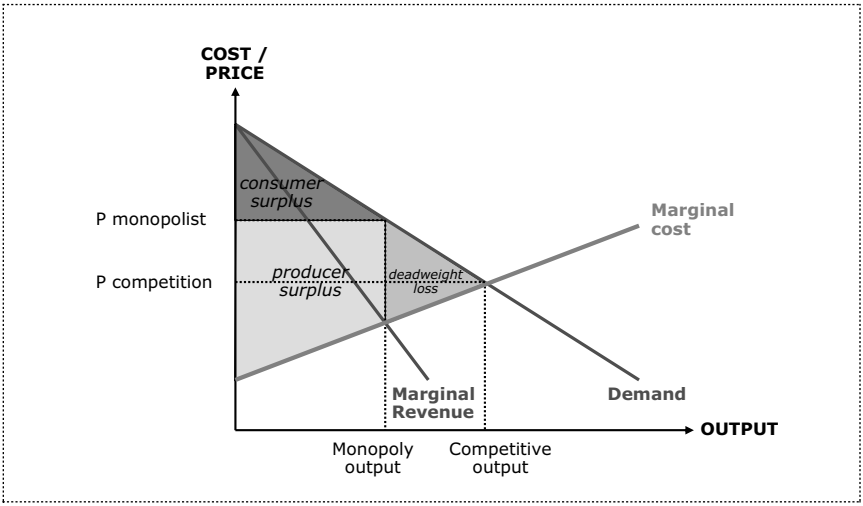

Figure 5.1/1: Efficiency loss resulting from a monopoly [Mask00,30]

This means that IP legislation accepts some **static inefficiency** (i.e. copyrighted goods may not be distributed as widely as is ideally feasible) in the interest of positive **dynamic effects** (i.e. in the interest of providing incentives for the creation of intellectual goods) [BeRa91,5]. Through monopolistic rents, inventors can appropriate returns on their work, resulting in innovations in the market. The gain in dynamic efficiency due to the increase in innovation is intended to compensate for losses from static inefficiency due to the under-utilisation of the knowledge protected by property rights [Arro62,616-617].

Apart from these inefficiencies, it must be taken into account that property rights are not free. The legal recognition of such rights frequently entails significant **transaction costs** that refer to all impediments to efficient contracting, including the costs of establishing and enforcing the property rights regime [Alle91,1]. Transaction costs also reduce public welfare, and should not exceed the eventual benefits derived from property rights [GoBo00,195-196].

The optimal property rights constellation therefore involves minimising the sum of economic inefficiencies and transaction costs. This is illustrated in Figure 5.1/2:

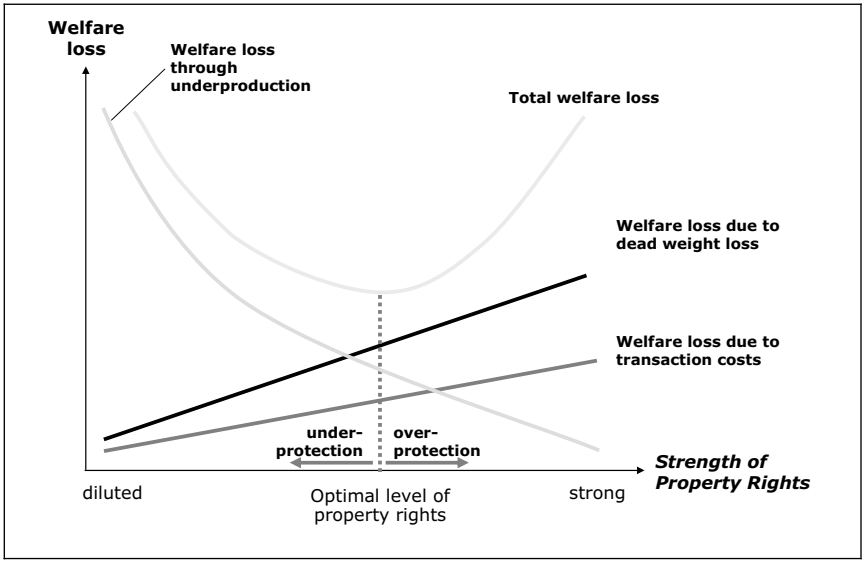

Figure 5.1/2: The welfare-protection trade-off

In an information society, the determination of an optimal level for property rights is extremely important. Since 1960, considerable theoretical research has been done regarding the economics of IP protection [Stig61;Arro62]. It is naturally extremely difficult to determine such an optimal level and to implement it in codified law by aligning the scope of IP provisions. In order to balance the costs of public policy options against the benefits, it is necessary to quantify welfare drivers such as gains or losses resulting from enhanced or reduced consumer privacy, and to perform complex interpersonal utility comparisons [Kins01,13]. The problems of operationalisation and the measurement of welfare effects also add to the difficulties of econometric research.

The issue of the general desirability of copyright, referred by Merges [Merg95] as the "grand question", has been settled in favour of copyright. The notions of "thin" and "thick" copyright represent different copyright paradigms. **Thin copyright** is a minimalist approach, where works are given only as much protection as necessary to encourage creativity, with the objective of making works widely available to the public. In contrast, **thick copyright** is a maximalist approach, which aims to maximise profits for content

6 Conclusion and recommendations

New technological trends such as the ubiquity of digital information, the widespread use of the Internet and increasing technical literacy have a significant impact on the commercialisation of IP and on society as a whole. New ICT offers both advantages and disadvantages to media companies, a situation referred to as the "digital dilemma". The key advantages are the opportunities for cost-efficient distribution and the development of progressive business models. The disadvantages are the ease of infringement and the difficulty of enforcing property rights.

It is difficult to provide a clear answer to the question as to how media companies should react to these developments. The issues are complicated by the diversity of the stakeholders concerned and the complex interrelationships of technology, economics and law. It is particularly important for media companies and policymakers to make a balanced assessment of all of the stakeholders and forces involved.

Stakeholder groups have extremely diverse, almost antagonistic, interests, motivations and values. Media companies and public policymakers should be cognisant of the diversity of stakeholders and forces involved, in order to introduce additional strategic options for dealing with the relevant issues. The development of DRMS solutions that are accepted in the marketplace depends upon a co-operative approach involving harmonisation of the interests of a large number of stakeholders that have conflicting objectives. Unilateral initiatives on the part of media companies, without the agreement of the consumer electronics industry, where the focus is solely on security mechanisms, have little prospect of success. Indeed, the continuing downturn of the DRMS industry could be explained in this light.

Furthermore, the issues must be considered and analysed from an economic, technological, legal, ethical and social perspective. It seems clear that the problem of content protection in the digital era cannot be scrutinised solely from a technical point of view or from any other single perspective. A broader, multidisciplinary framework is necessary in order to deal with the complex issues involved.

It can be concluded that the most effective mechanism for deriving value from digital intellectual property involves a combination of technical, legal and structural strategies that are balanced in a DRMS installation. Whether or not a particular DRMS is successful in the marketplace depends not only on its level of protection but also on the business models it supports and the legal framework

8 Index