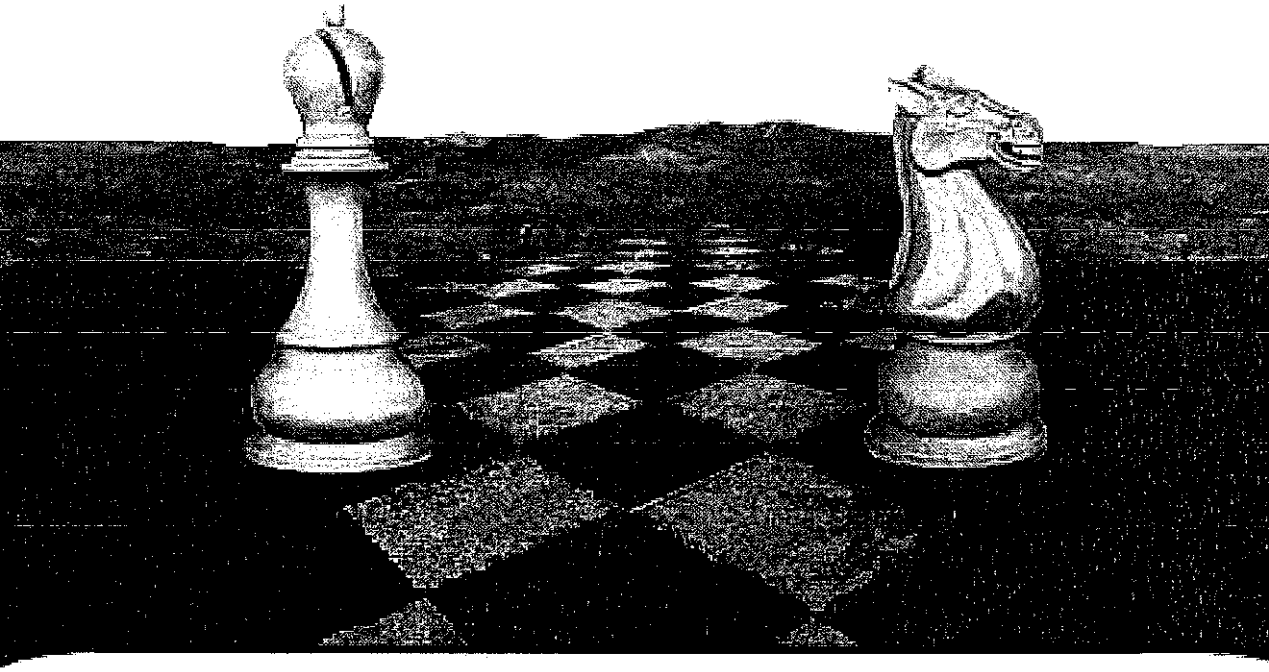
MASTER

Developing a patent strategy for Philips' Digital Rights Management patent portfolio

van de Laarschot, H.U.O.N.

Award date:
2003

TU/e technische universiteit eindhoven



Developing a Patent Strategy for Philips' Digital Rights Management Patent Portfolio

H. van de Laarschot

---------- CONFIDENTIAL UNTIL DECEMBER 2005 ----------

Developing a Patent Strategy for Philips' Digital Rights Management Patent Portfolio

by Huon van de Laarschot
(student ID 449498)

September 2002 - November 2003

Written under the direction of:

M.S.C. Bakker LL.M. Ph.D.
Eindhoven University of Technology
Department of Technology Management

And

A.A.C.M. Kalker Ph.D.
Eindhoven University of Technology
Department of Electrical Engineering

And

A.P. Engelfriet M.Sc.
Philips
Intellectual Property and Standards

"Developing a Patent Strategy for Philips' Digital Rights Management Patent Portfolio"; a thesis submitted to the "Technische Universiteit Eindhoven" (Eindhoven University of Technology), The Netherlands; in partial fulfilment of the requirements for the degree of Master of Science in the "Technology and Society" program (specialisation: Technology and Innovation Policy for Advanced Economies, Computer Science) at the department of Technology Management.

ISBN 90-9017652-7

Summary

A patent strategy aids a company in strengthening its position amongst other patent holders. General strategies focus on licensing to create revenues, focus on isolation to offer a unique product (feature) or defend against the strategy of other companies. Which strategy to follow depends on the willingness to license and the importance of a company's portfolio. Other factors that influence strategy choice are market specific (e.g. number and type of competitors) and technology specific (e.g. multi-invention technologies). Factors such as the emergence of standards and the size of a company also influence this choice. As a patent strategy is used within a company amongst other strategies (e.g. market strategy), this strategy must be combined with those other strategies.

In a case study of patent portfolios for DRM technologies, Philips patent strategy is determined. In order to do so, DRM patents are defined and then searched for using the Micropatent, Pluspat and Espacenet patent databases. A DRM patent is defined as " *a patent on a technology or the use of a technology for managing interaction with digital content according to interaction rights*". Several enabling technologies, such as watermarking, fingerprinting and encryption, can be used in DRM and a patent on the use of such technologies can constitute a DRM patent.

A search is conducted for patents that contain keywords that are typically used in DRM patents. Several steps are taken to improve the completeness of the result set and the results are then filtered to remove non-DRM patents. This filter method uses the European and International patent classifications, to leave only those patents that have been assigned classes that are likely to hold DRM patents.

The DRM patents that are found give an indication of which companies hold relatively large DRM patent portfolios. These companies, their portfolios and their relation to several DRM alliances are compared. The most important portfolios are held by InterTrust and ContentGuard. Both Philips and Sony, which have a history of forming alliances to push certain technologies (e.g. CD and DVD), hold an above average importance DRM patent portfolio. Most other companies that are included in the comparison (e.g. Hitachi, IBM, Matsushita and Thomson), hold diverse portfolios that do not focus on specific technologies.

The comparison shows that access to InterTrust's patents and to a lesser extent some of ContentGuard's patents is essential and that DRM patent holders, specifically those in the consumer electronics industry, need to cooperate in order to be able to use DRM technologies. Philips patent strategy should be a combination of a licensing and a defensive strategy, in order for Philips to exploit the value of the patents it holds and in order to defend itself from being excluded from using DRM technologies. Furthermore, standardization efforts are important for DRM to be successful and it is critical that Philips promotes the emergence of a (dominant) DRM standard that it finds beneficial. Based on Philips' position amongst other patent holders this could very well result in an (industry) effort to standardize DRM lead by Philips and one or more other consumer electronics companies (specifically Sony).

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

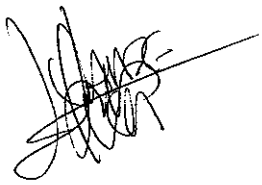
In the year 2000 the European Patent Office estimated there were over four million patents and licensing revenues had grown ten-fold since 1990 to over 100 billion dollars worldwide[1]. These figures show how important patents have become, not only for the appropriation of an invention, but also for generating revenues. The role a patent fulfills is changing from a tool aiding an inventor in protecting his or her work, to a business tool. The use of patents is becoming part of a business strategy and as such planning the creation and exploitation of patents is becoming ever more important.

Writing this paper about patent strategies has been an eye-opener for me, as it has shown me how diverse, intellectually stimulating, yet practical, research in the field of patents can be. To most, it would seem to be the exact opposite as such research requires enormous heaps of data to be reviewed, the understanding of technical documents and to some extent a resistance to "legalese". To me this posed as much a challenge as an opportunity to explore different fields of research and combine knowledge from these fields.

Many people have supported me in performing this research and writing this paper. I particularly wish to thank Martijn Bakker, for the discussions we've had about the value of patents to a company, these have been very helpful; Arnoud Engelfriet, for sharing with me so much knowledge about Philips' IP operations; and Ton Kalker for sharing his technical expertise. Research for this paper took place both at Philips Intellectual Property and Standards (IP&S) and at the Eindhoven University of Technology. I'm grateful to Philips IP&S and in particular its CEO, Mr. Peters for giving me the opportunity to perform part of this research within the company.

Furthermore, I wish to express my eternal gratitude towards my parents; they have always supported me and without them, I would not have been able to pursue as many of my dreams as I have been able to pursue. In addition, I wish to thank my girlfriend, friends and family, all of whom have been there for me whenever I needed them.

This paper is the result of true enthusiasm for the research topic. I hope that you will enjoy reading it and I welcome all comments, questions and such.



Huon van de Laarschot - Eindhoven, November 19th 2003

[1] Source: www.european-patent-office.org/epo/facts_figures/facts2000/e/5_e.htm

THIS PAGE INTENTIONALLY LEFT BLANK

Index

1 Introduction

This introductory chapter provides an overview of this research paper and it includes a discussion of the research goal and the research questions, which explain the relevance and the intentions of this research.

Contents of this chapter:

1.1 Research Goal

In a world where the innovativeness of products is crucial to a company's success, the right to stop others from manufacturing, using or selling an invention that is granted by a patent right is becoming ever more important. Companies continually invest a considerable percentage of their revenues in research and development in an effort to stay ahead of the competition and patents are an important part of this innovation cycle. The creation, management and exploitation of patents is an element of a companies overall (business) strategy of ever increasing importance.

As a large, multinational and innovation driven company Philips has recognized this growing importance of patents and as such has placed all of its intellectual property and licensing operations in a single business group: Philips Intellectual Property and Standards (IP&S). One of the many patent portfolios that Philips IP&S manages is Philips' portfolio of patents on Digital Rights Management (DRM). Although the scope of DRM is explained in detail in this paper (see Chapter 3), DRM can in general be described as technologies aimed at technically regulating interaction of electronic content[2], such as usage and distribution. These DRM technologies are expected to become of great importance to the consumer electronics products that Philips and other companies produce. As a result, patents on these technologies will be of great importance as well. This calls for Philips to plan as much as possible the creation, management and exploitation of DRM patents or in other words to develop and follow a patent strategy.

The research goal therefore is "to strengthen Philips' position amongst other DRM patent holders, by developing a strategy that guides the creation, management and exploitation of Philips' DRM patent portfolio". The actual implementation of the strategy and, for example, organizational choices that have to be made to implement the strategy are not part of this research. Making those choices requires detailed knowledge about Philips intellectual property operations that Philips, like any other company, will not disclose publicly.

1.2 Research Questions

Developing a patent strategy requires that a lot of information is gathered, ranging from knowledge about the structure of Philips' DRM patent portfolio to details of the relationships between Philips and other companies holding DRM patents. Together this information enables the research question to be answered: "What patent strategy should Philips choose for its DRM patent portfolio, based on the composition of this and other companies' portfolios?" In answering the research question the methods that are used are thoroughly discussed to make this research a model for answering patent strategy questions in general. As the research focuses foremost on patent strategies, the technology choice (DRM) and the company choice (Philips) should be seen as a case study.

---

[2] The phrase "content" indicates a work (such as a text or an image) and not the embodiment of that work (such as a book or a JPEG file).

Several steps are taken to gather the information necessary to answer the research question. Each of these steps is dealt with in a separate chapter and this is an overview of these chapters and the questions they deal with:

Chapter 2: Patent Strategies - This paper is about patent strategies and as such, literature on these strategies has to be explored: What patent strategies are there in general and what factors influence the choice for a strategy?

Chapter 3: Defining DRM - The patent strategy is developed for Philips portfolio of patents covering Digital Rights Management technologies: What is Digital Rights Management and what should be considered a DRM patent?

Chapter 4: Searching for Patents - There's no list available of DRM patents and therefore such a list needs to be created: What methods can be used to find DRM patents?

Chapter 5: Comparing Companies and Their Portfolios - The results of the search for DRM patents can be used to find and compare the portfolios of DRM patent holders. What companies hold important DRM patent portfolios and how do these companies and their portfolios compare?

Chapter 6: Determining the Strategy - The answers to the four questions in the previous chapters provide the information needed to formulate a patent strategy for Philips: What factors are decisive in choosing a patent strategy for Philips?

1.3 Additional Comments

There are three main issues that have an effect on this research and are therefore discussed in this introductory chapter. First of all this research deals with a delicate subject, as companies are extremely careful when disclosing information about patents, licensing and patent or research strategies. Secrecy is essential in many cases as the strength in negotiations largely depend on having more information than the opposite party has. As a result there's little immediate information available about which patents a company considers part of its DRM patent portfolio, whether or not a company is interested in patenting DRM technologies, which patents are licensed and what settlements are made when a patent is infringed. As such it is impossible to gather quantitative data that can be used for statistical analysis and therefore, this research is of a qualitative nature.

The second issue in performing this research is that there is a lack of existing publications on patent strategies [Somaya, 2002b]. This is overcome however, as there are many publications on related aspects (e.g. patenting and licensing). Chapter 2 discusses this issue in more detail.

The third issue is that DRM technologies have only recently been developed and have not been widely implemented yet. There are therefore still many uncertainties about these technologies and about what a DRM system will generally look like. In this research this is dealt with by looking at the essence of DRM in defining a DRM patent and separating a DRM technology from a DRM enabling technology. When at a later stage of the development of DRM products it becomes evident what technologies are dominant in the design of DRM systems, this research is still of value as it can be complemented with new research to create a new strategy.

2 Patent Strategies

It is necessary to explore the domain of patent strategy research in order to create an understanding of the questions that are involved in this research. This exploration shows there are several generic patent strategies. To determine which of these patent strategies to choose requires that several factors be analyzed.

At the end of the chapter a model is presented that guides the choice for a patent strategy.

Contents of this chapter:

2.1 Research on Patent Strategies

2.1.1 Comparison with Existing Research

Research on patent strategies covers the three strongly connected areas of patenting (acquiring an exclusive right to exploit an invention), licensing (granting others certain rights towards exploiting the invention) and enforcement (legal actions based on the exclusivity of a patent right) [Somaya, 2002b]. In research where the perspective of patenting is subjugated to the perspective of innovation in a larger context, there is often an overlap with other research fields, such as microeconomics [e.g. Kauko, 2000], macroeconomics [e.g. Gallini, 1984] or research on a specific technology [e.g. Pakes and Temin, 1991]. Most often in such research, the focus is on only one of the patent research areas, with a preference in literature for patenting and enforcement. It is relatively easy to get access to data necessary for such research, although obtaining such data is still very time consuming.

This paper researches patent strategies from a combined perspective of the role of a company's patent portfolio for a certain technology and the relation this company has to other companies holding patents to the same technology. It covers all three areas of patenting, licensing and enforcement, yet unlike most existing research papers, it does not treat these research areas as autonomous fields of research. Instead, this paper considers the strategic choices made within a company about patenting, licensing and enforcement a set of nested choices that require attention as a single strategic question, not as consecutive choices that are made independently of each other. To clarify, some typical research questions in each of these fields are compared to questions that are explored in this paper.

- Patenting as an autonomous choice: What company structure enables a maximum number of inventions made in research divisions to be turned into patents?[3]
- Licensing as an autonomous choice: How can licenses be valued and priced to achieve optimal revenue for the licensor?[4]
- Enforcement as an autonomous choice: Is there a correlation between the outcome of enforcement lawsuits (e.g. plaintiff wins, defendant wins or settlement) and the financial strength of the companies involved?[5]
- Patenting, licensing and enforcement as a single strategic question: How can company X produce a certain product that requires company Y to provide a certain license?

The example given of a single strategic question is very broad in its scope. It is possible to focus such a strategic question on one of the three areas of patent strategy research, yet such a question will inevitably be linked to questions in the remaining two research fields.

---

[3] For a study on patenting see Hall and Ham (1999)

[4] For a study on licensing see Rockett (1990)

[5] For a study on enforcement see Lanjouw and Lerner (1997)

2.1.2 *Nested Choices in Patent Strategy Research*

As mentioned, the three research areas in patent strategy research are related and as a result the choices available in one field, for example licensing, depend on the choices made in another field, in this case patenting. The easiest way to understand this phenomenon of nested choices is by giving an example that relates these choices in each field. Below is an overview of *some* of the options for patenting, licensing and enforcement.

Options in patenting:

1a. Patent an invention
1b. Do not patent, but keep an invention secret (trade secret)
1c. Do not patent, but publish an invention so no one else can patent it

Options in licensing:

2a. License so other companies can produce the complete product themselves
2b. Provide other companies with the patented parts (e.g. chips) without allowing them to produce these themselves
2c. Do not license at all

Options in enforcement:

3a Enforce patents in order to stop infringement
3b. Enforce, but if possible settle claim
3c Do not enforce at all

If option 2a or 2b are chosen, then option 3a poses a risk if the infringing company also licenses some of its patents to the enforcing company. The infringing company could file a counter lawsuit claiming infringement of one of their patents. This could then turn a moneymaking opportunity into a costly legal mess for both companies.

Option 1c completely eliminates licensing opportunities and option 1b (virtually) eliminates option 2a. Choosing option 3c has an effect on choices made in patenting, as a repetitive choice not to enforce infringement can diminish the value of a patent portfolio. The value of a patent will than be similar to the value of publishing the invention to prevent others from patenting it.

Many more relevant choices are included in this process of making nested choices. In licensing, for example, the type of license that is provided is a major issue and the different types of licensing strategies that can be followed are dependent upon the patenting strategy that has been followed. The different patent strategies that are available are discussed in this next section.

2.2 Generic Patent Strategies

In literature on patent strategy research, three patent strategies are often mentioned as "generic" [Somaya, 2002b]. These three strategies cover the use of patents: (1) to defend against imitation, this is called an isolation strategy; (2) to derive value from licensing these patents, this is called a licensing strategy; and (3) to defend against other firm's patent strategies, this is called a defensive strategy. Some literature also mentions a market valuation strategy, in which the role of patents is to demonstrate innovation or to build an asset base [e.g. Hall et al, 2000]. All four of these strategies are considered generic patent strategies in this paper and a more detailed discussion of these strategies follows. It is worth mentioning that these strategies cover the different motives of companies as to "why they patent" [Cohen et al, 2000]. However, patenting is not the only method used by companies for appropriation. Lead-time advantages, secrecy and complexity are used more often than patents[6] [Arundel, 2001].

2.2.1 *Isolation Strategy*

An *isolation strategy* is focused on protecting a firm's core assets and is often coupled with a legal strategy to guard against imitation. Such a strategy typically protects the inventions used in products that put a firm in an advantageous market position. Typically, follow-up innovations will be protected as well in an isolation strategy An isolation strategy is also often employed by new entrants to a market that are looking for growth in this market based on the innovativeness of their product. Such a strategy allows new innovative entrants to keep existing companies, which will often have much better organizational resources (e.g. sales channels), from directly imitating them. This "buys" the entrepreneurial company time to invest in and enhance its own organizational resources, so it can better withstand competition.

The core features of an isolation strategy for each of the three research areas in patent strategy are:

Patenting: Protect the invention in the best ways possible. This typically consists of creating a 'patent thicket'; a series of related patents that cover different features of the invention and often production methods as well [Merges, 1996] [Bessen, 2003]. The goal of this patent thicket is to prevent a competitor from being able to 'invent around' a patent (i.e. to use different technological implementations that avoid patent infringement, yet yield a similar product as the patented invention). A similar method is the creation of a "wall" or "cluster" of patents that covers every commercially viable variation to an innovation [Davis, 2002]. It is of course of the utmost importance that no other companies hold patents that are essential to being able to follow an isolation strategy for a certain product or technology.

[6] Likely such method are often used when patent protection is not available or patent infringement would not be detectable.

Licensing: The strategy here will simply be not to license at all. This can be difficult when large cross-license programs are in place between companies and therefore often requires special attention in licensing contracts (e.g. every license a company offers can include a section that explicitly states which patents are never licensed).

Enforcement: The success of an isolation strategy depends on the ability to prosecute infringement. If infringement cannot be easily detected, there is no reason to follow this strategy [Crampes and Langiner, 2002]. Furthermore, it requires that the patent holder is able to spend large amounts of money (often upwards of 2 million $) and a great deal of time (often over 2 years) to enforce a patent by going to court [Somaya, 2002a]. Companies that do not enforce their patents can easily be seen as 'pushovers' by other companies, dramatically limiting these companies' power. Financial ability to prosecute is not the only concern for a company, for instance when the company infringing the patent and the company enforcing the patent have existing business relations (e.g. existing licensing programs or partnerships). In such cases, the willingness to enforce a patent right might be low within the company holding the patent, as it could have unwanted repercussions.

An isolation strategy is very costly, due to the number of patents needed to protect an invention[7] and the high litigation costs to protect against infringement. The main concern for a company using an isolation strategy will be, whether the benefits of being the only company to offer a certain patented product (feature) has more financial and other benefits than licensing this same patent. It is not easy to determine the possible licensing value of a patent and it is even more difficult to estimate what non-financial consequences it has being the only company that can offer a certain product. An isolation strategy is not used very often because of the costs and the uncertainties involved. Typically the strategy is used in single-invention products, where it is likely that one company holds all the necessary patents (e.g. medicine, electric shavers and coffee makers).

A final remark about an isolation strategy is that often such a strategy is aimed at protecting a certain product and not necessarily the patented technology itself. Therefore licenses can very well be granted for the use of a patented technology if there are multiple products in which it can be used and some of these products are for instance not produced by the company owning the patent.

[7] The cost lies not only in patent fees, but also of course in research.

2.2.2 *Licensing Strategy*

A *licensing strategy* is focused on exploiting the economic value of an innovation by creating revenues through licensing. Such revenues are however not always incurred directly, such as, for example, when cross-licensing is used[8]. This strategy can be seen as the exact opposite of an isolation strategy. In literature it is often mentioned that the patents that are licensed under a licensing strategy cover non-core technologies, technologies to which several alternatives are available and technologies that the licensor is not using in or are not critical to its products [Somaya, 2002b]. In multi invention products (e.g. consumer electronics), it is virtually impossible to license only these types of technologies. In order to make such a multi invention product, licenses are needed from several companies and these companies will want to receive licenses in return for the licenses they grant.

An important aspect of this strategy is determining the value of a patent in order to come up with a pricing strategy for the licenses. It can be difficult to directly calculate such value as most often the value of a patent cannot be determined on a cost basis. This is due to the fact that research and development activities cannot always be quantified in monetary value and do not always result in patents that can be licensed. Often an indirect approach is used to determine a pricing strategy. Hereto the prices of licenses to alternative technologies are examined and the extra value that the patented invention offers for the buyer is estimated. As a company sells licenses to its patents as well as purchases licenses it needs, a company will try to maximize revenues by making more money on the licenses it sells than it has to pay for the ones it needs.

A development worth mentioning in the context of this discussion on licensing strategies is that during the last few decades some firms have emerged that generate revenue solely from licensing patents to technologies they've developed[9]. These firms do not cross-license, as they have no use for such licenses, because they do not produce any products themselves. Therefore, such firms cannot be persuaded to lower the price for a license or change the license terms by threatening not to license certain technologies to them, a method often used when companies holding mutually important patents negotiate licenses.

---

[8] Although a licensing strategy can include cross licensing, it is different from a strategy that involves cross licensing as a defensive strategy. The primary goal of a licensing strategy is to patent technologies that could generate revenue through licensing, while the primary goal of licensing in a defensive strategy is to force other patent holders to negotiate cross-licenses.

[9] An example of such a company is Dolby, whose revenues are based on the licensing of its more than 600 patents on, for example, audio technologies. InterTrust is an example of such a company that holds patents to DRM technologies. This company will be discussed in more detail in this paper.

As such, these firms tend to have a strong position in demanding high licensing fees. Assuming of course they have patented technologies that are in high demand, such as unique technologies (i.e. there are no substitutes available) or technologies that are essential to a standard[10] (i.e. it is impossible for a product to adhere to the standard without infringing this patented technology).

In a similar position as the aforementioned license-revenue based firms are individual inventors and non-profit research related institutions (e.g. universities). It is less likely that these institutions would misuse their position, as they are generally not focused on profit maximizing. Individual inventors typically do not have the necessary resources to search for product infringement[11].

The core features of a licensing strategy for each of the three research areas in patent strategy are.

Patenting: Unlike in an isolation strategy is not is there if there already are several other companies that hold patents on complementary technologies. In fact, this could indicate that the technology is (expected to be) in great demand. However it is critical to the value of a patent that few technologies exist that are similar to the extent that they can replace the patented technology that will be licensed.

Licensing: In a licensing strategy the main goal is to extract as much value from a patent as possible. This will typically mean that profit maximization is strived for, but this does not necessarily mean that selling licenses is focused on short term gains only. In some cases selling a license cheap to push a technology and enable it to become a standard or dominant design can result in greater profits in the long run (e.g. Philips and Sony pushing their compact disc technology).

A licensing program that is set-up does not necessarily aim at selling licenses, equally important can be cross-licensing. Often the company that wants to license a certain patent also has an interest in licenses to technologies the other company has to offer. This can result in a cross-licensing program where no money changes hands. Often however, one company has more to offer than the other in a cross-licensing program, in which case the company licensing the more valuable portfolio will still seek monetary compensation for the additional value it is offering.
To compare these patent portfolios companies typically use a so-called 'proud list'. This is a list that the companies that want to cross-license prepare with a certain number of their most important patents relevant to the technology they're cross-licensing. The number of patents in this proud list is a number they have agreed upon prior to constructing the list, typically this number is somewhere between 20 to a 100 [Teece, 2000].

---

[10] Licensing terms that patentees are offering can influence the process of setting standards. The process is as such not about finding the best technical alternative, but also about finding the best financial, yet technically adequate, alternative. In certain standard setting bodies, it is customary to ask patentees to forsake their rights and give up their claims. This can be the case if a standard becomes a legal standard, enforced by (national) law.

[11] The probability of being involved in a lawsuit involving patent infringement is however larger for individuals and smaller firms [Lanjouw and Schankerman, 2001].

Enforcement: The goal of a licensing strategy is to exploit the economic value of a patent. Deciding on whether or not to enforce a patent will therefore most likely be a strict financial decision. Companies infringing upon a patent will be sued for monetary damages and often a case is settled if the company is willing to purchase a license. The threat of a lawsuit can lead to an increase in the value of a license especially when production has started. A company might be willing to pay more for a license if its other options are to go to court or stop using the patented technology altogether than when it has a choice between different technologies prior to starting production.

2.2.3 *Defensive Strategy*

A *defensive strategy* focuses on shielding a firm from the outcome of the patent strategies of others. The most common element of a defensive strategy consists of "patenting around" another firm's technologies. This creating of patents that are similar and sometimes complementary to inventions patented or in development by competitors typically serves two goals. The first goal is to create the freedom needed to operate or in other words to create a safety net of patents that prevents the competition from effectively using an isolation strategy. The second goal is to create a "patent barrier" for the competition that can be used to limit the options the competition has. Both types of defensive strategies are discussed below.

Freedom-to-operate: Cross-licensing – This strategy consists of offering a company only a cross-licensing program for patents on a certain technology. This doesn't necessarily have to be an exchange of licenses for a single technology. It is entirely possible to exchange licenses for unrelated technologies. This strategy is most important in electronics [Teece, 2000], where a single product can be covered by several hundreds of patents. It is often impossible to identify each and every single patent to which a license is needed. It is easier to identify the companies that are likely to own these patents. By following a defensive strategy it is likely that some patents are created that are important to some, possibly all of these companies. Such patents can then be enforced when leverage is needed in a dispute regarding other patents or even some non-patent related dispute.

Patent barrier: Blocking a competitor's technologies – Unlike the previous strategy where blocking a competitor's ability to produce a certain product is used as a threat, this strategy is aimed at blocking a competitor from making a certain product altogether or from being able to effectively exploit a patent (e.g. by withholding related or follow-up patents). Such a strategy inevitably leads to repercussions and should therefore be used with caution. A typical use would be in a standard setting process, where the stakes are high as the outcome will determine which patents will become essential and therefore, most likely, very valuable. A defensive strategy can then be used to force access to a market that would otherwise be closed off by another company's patent strategy.

In complex industries such a defensive strategy is dominant in forcing competitors to negotiate in order to obtain a license [Cohen et al, 2000]. Yet such negotiations could also cover the price of a license and a defensive strategy can then be used to prevent other companies from being able to extract exorbitant royalties.

The danger of this strategy, as mentioned, lies in the possible repercussions, which are most likely of a similar nature. This can lead to a mutual hold-up, where two companies are blocking each other's use of a certain technology. Some companies therefore choose a mutual non-aggression strategy [Bessen, 2003]. It is important to realize that these strategy elements are of no use when dealing with individual inventors and patent-only companies.

The core features of a defensive strategy for each of the three research areas in patent strategy are:

Patenting: The focus should be on finding out what technologies are of importance to competitors and patenting as many relevant inventions in that field. Although this sounds easy, it can be quite difficult understanding what technologies the competition is interested in. Looking at their patenting behavior is an easy way, yet this method delivers results that lag approximately two years behind, as there is a delay between the patent application and the publication of that application.

Licensing: If a defensive strategy is focused on creating freedom-to-operate, cross-licensing will be a major component of the strategy. If the strategy is focused on blocking a certain technology or competitor then licenses will typically never be granted.

Enforcement: Patents provide power in a defensive strategy through their legal status Enforcement is therefore a critical aspect of this strategy, requiring any company that wishes to follow this strategy to invest time and money in possible litigation.

If all else fails, there are at least two more methods to defend against another company's patents. These methods simply consists of using the legal measures available, which generally are (1) going to court to invalidate the patent or (2) using anti-trust laws to force the patent holder to license the patent. Both options are costly, time-consuming and typically unfit for a fast-paced industry such as the electronics industry. As such, these options should be used only as a last resort.

2.2.4 *Market Valuation Strategy*

A *market valuation strategy* is aimed at increasing the market value of a firm by increasing the number of patents a company has [Hall, 1999]. Such a strategy is often implemented by start-up firms or rapidly expanding firms that need capital and feel their valuation is based on their patent portfolio. Another scenario in which this strategy is implemented is when firms are looking to be acquired by another firm or wish to merge with another firm and desire to increase their (stock-) value.

When start-up companies apply this strategy, it should be seen as an added strategy aspect to one of the other patent strategies. The value of a start-up company will be judged based on the ability to license or sell their patent portfolio or on the ability to use it in an isolation strategy. In the electronics industry all companies that are not start-ups generally hold several hundreds to thousands of patents and this strategy is therefore not used in this industry. As such this strategy will not be discussed in any more detail.

2.3 Market and Technology Factors in Patent Strategies

Generic patent strategies cover a wide array of options a company has in matching its market strategy with a strategy of patenting, licensing and enforcement. When dealing with certain technologies or certain markets however, there are more subtle details to these strategies. Firms in the pharmaceutical industry generally adopt an isolation strategy, so do many firms with an e-commerce focus (e.g. Amazon through its much discussed and often disliked one-click patent[12] and to an even greater extent a company such as Priceline.com[13]). The pharmaceutical firms tend to patent several smaller inventions related to product innovations as well as process innovations that are related to a newly developed medication. The e-commerce firms tend to patent one broad automated process, which entails the back-end and front-end off the online service they want to offer.

---

[12] The validity of this patent [US Patent number 5,960,411] has become very doubtful after "the US Federal Circuit court of appeals [...] dissolved the preliminary injunction that [...] kept barnesandnoble.com from offering its Internet customers the one-click shopping that Amazon.com offers" [Stern 2001]. This however does not influence the fact that Amazon tries to create a service this way that only they can offer.

[13] Priceline.com has a patent [US Patent number 5,794,207] on the reverse auction model ("name your price" model). This patent covers what is perhaps Priceline.com's most important selling point. Even though Priceline.com finally settled a lawsuit against Microsoft's Expedia.com alleged infringement of the patent, Priceline.com pursued an isolation strategy for many years against Expedia and likely still does against other competitors.

These subtle differences within the same type of general strategy are related to both the nature of the technology and the nature of the market that is concerned. In the pharmaceutical industry, there are many ways to circumvent a patent by applying a different production method. Furthermore, the costs of developing a medication are enormously expensive and this calls for a greater investment in protecting this invention by patents. In e-commerce, the invention is often merely the transfer of an existing process to the realm of the Internet and there is little research investment involved[14]. This results in the effect that most often only one patent can be filed for a specific e-commerce related invention[15].

To understand patent strategies in the electronics industry it is necessary to understand such market and technology factors as well. The next two sections discuss these factors in detail.

2.3.1 *Market Factors*

For the markets in consumer electronics that Philips is in, there is one issue that is of major importance in deciding what patent strategy to use. This issue is the ongoing convergence of personal computers and audio/visual consumer electronics[16]. Computer technology has rapidly progressed, changing the role of a computer from a business machine for professional use in several steps to a multimedia entertainment center for home use. Most of the functions that 'classic' consumer electronics for the home fulfill, can now also be fulfilled by multimedia computers, such as, for example, listening to music or watching a movie. Add to that the increasing number of computers that are used for (broadband) Internet access and you get a technology that is able to offer more than typical consumer electronics.

Until now, the price of computers and the size of them have made the computer an inadequate replacement for CD players, DVD players and the like. Computers are over-equipped multi-purpose devices and are therefore too expensive to replace multiple single-purpose devices. This is where the increasing interconnectedness of computers plays its part. More and more a computer can be connected with different existing home audio/video appliances, such as TV's, stereos and such. At that point, they can be connected to existing systems and there is no need anymore to have both a computer 'upstairs in the study to work and downstairs in the living room to watch TV'.

---

[14] Even if software needs to be made to offer a new service that is covered by a patent, the part of the investment that is strictly related to this new service is often minimal when compared to the software investment of enabling online business in general. Furthermore, such investments are by far no match for research and development costs in the pharmaceutical industry.

[15] As many e-commerce companies are start-ups, the choice to apply for a single broad patent could also be a cost issue.

[16] Audio/visual consumer electronics will be referred to as consumer electronics or CE.

Furthermore, some new appliances, for example most portable MP3-technology based audio devices, can only be connected to computers, not to classic appliances such as CD players. The general idea of all this is that the computer will play a central role in providing audio/visual entertainment in the modern home.
It is likely that this "digital convergence" [Yoffie, 1997] will result, to some extent, in a convergence of some of the markets that computer manufacturers and consumer electronics manufacturers serve. This convergence can result in a model of one central hub, the computer, and several 'dumb' displays and input devices; or a model without a hub, but with several 'smart' displays and input devices. No matter which model or combination of models pervades, it is obvious that consumer electronics companies face new competition.

This convergence is of major importance, because adding DRM technologies to electronic devices and computers brings these devices further together. This is due to the necessity of compatibility of DRM systems. It would be unacceptable if there are too many incompatible DRM systems around and consumers would therefore not be able to use the same content on both their computer and their home entertainment system. This requires that there will be an overlap in the type of DRM technologies used by computer manufacturers and consumer electronics manufacturers. Electronics companies therefore fear that they could become dependent to some extent on their new competitors, the computer software and hardware manufacturers[17], if these own patents on DRM technologies that are needed to produce compatible DRM appliances.

2.3.2 *Technology Factors*

DRM technology is new, innovative and has been employed only on a very small scale. Therefore it is impossible to gather empirical evidence of the efficacy of different patent strategies through the analyses of quantitative economic indicators. Instead the problem of determining which patent strategy Philips, regarding its DRM patent portfolio, should pursue, shall be approached by qualitatively determining the adequacy of different strategies. This approach consists of a review of DRM patent portfolios of Philips as well as its main competitors and a limited number of other DRM patent owners. Based on relations between patent portfolio size and compatibility and based on market strategies of some competitors, as far as these are evident, the relative strengths and weaknesses of each company's portfolio will be analyzed.

[17] It is important to realize that what makes up a computer is as much the hardware as the software. Electronic devices are becoming more like computer systems, as they too now use standardized hardware and the addition of software offers certain features. This means the importance of DRM patents held by software manufacturers is likely to grow.

Products using DRM technologies will be multi invention products, as DRM can combine (patented) technologies from fields such as watermarking, encryption and copy protection. In the next chapter, where DRM is defined, this multi invention character of DRM will be featured in more detail (see Chapter 3). The effect of this multi-invention character is that it is very unlikely that a single company will hold all the patents needed to produce a complete DRM product. This doesn't necessarily mean that an isolation strategy is impossible however, as several companies could team up and still try to isolate themselves from their competitors.

2.4 Additional Factors

There are more factors that are of importance in determining what patent strategy to use. The most important internal factor is the company size and the most important external factors is the emergence of standards. Both these factors are discussed below.

Internal factor: Large vs small companies - Large companies usually have multiple product lines and perhaps even different markets they supply to. These large companies will therefore often have a general patent strategy and a technology or market specific strategy. To illustrate this, Philips typically licenses all its patents to any company willing to pay, with the exception of patents on certain core products, such as its patents on shaving technologies.

Related to company size to some degree is the size of a company's patent portfolio. Companies holding a very large patent portfolio rarely license single patents, but instead license patents per technology or product. Such a license then covers all patents needed to produce that product or use that technology. This form of licensing simplifies an otherwise time consuming and unlikely fully accurate process of finding all relevant patents.

When producing multi-invention products, a company has to choose between an integrated and a non-integrated mode of production. In an integrated mode a company will strive towards obtaining all the necessary technologies and patents needed for the product. This means a company can acquire or merge with firms that hold patents or have the technology they need. Another option is for the company to come up with similar technologies as the ones patented by others. This integrated mode is more suitable for larger companies.

In a non-integrated production mode the technologies that are needed are obtained through licensing or the purchasing of components that embody the invention. The type of mode that is chosen to produce a product has an effect on the patent strategy that can be chosen. An integrated mode and an isolation strategy could work well together, but isolation might be more difficult in a non-integrated mode. Both small and large companies can use this non-integrated mode.

External factor: Standard / technology tie-in – There are several ways a standard can be set, of which the most important are:

(1) Several companies can set a standard through an organization set-up specifically to create standards for a certain (type of) technology. Such a market standard is voluntary, but being a member of this organization or adhering to these standards can have legal consequences. A standard can, for example, specify the use of a certain patented technology. The company owning this patent is most likely a member of the standard setting organization and will license only against certain terms.

(2) A governmental organization can set a standard and has the choice of making this a legal standard. Such legal measures force companies producing a certain kind of product to adhere to a technical standard.

Using a certain technology or adhering to a certain standard has a tie-in effect. The greater the dependency on a standard or technology, the more difficult it is to start using a different standard or technology. Choosing to use a technology or standard that is dominated by another company is potentially dangerous, as this provides leverage for this other company in demanding for example that such a standard will be changed or expanded to its benefit.

When a standard covers patented technologies that are owned by several different companies, a system called a 'patent pool' can be used to make licensing easier. A patent pool removes bargaining difficulties that are caused by overlapping patent portfolios [Lerner et al 2003]. In such a patent pool system, a company can purchase licenses to all necessary patents for a technology or a standard at once. A patent pool can promote the use of a standard.

Although by its very nature patent law enables a company, in some instances, to create a monopoly in a certain market, there are exceptions to the legal protection patents provide due to anti-trust laws. Yet these exceptions are very rare and are more relevant a company's market strategy than to a patent strategy. It is worth mentioning that the most important way to prevent creating even the slightest doubt about whether a licensing program is unfair is by using so called 'RAND' licensing terms. These are terms that are reasonable and non-discriminatory, basically meaning that each company that a license is granted to gets the same terms, that these terms are reasonable and that every company that accepts these terms will be granted a license.

2.5 Strategy Choice Model

In this last section of the chapter on patent strategies a model is presented that can aid in deciding what patent strategy to follow. As there are many factors that influence this strategy choice it is impossible to use all of them in a model because it would make the model too complex. The model therefore uses only two variables, which are related to many of the factors that were discussed in the preceding two sections. These variables are "the importance of the patents owned" and "the willingness to license"

These two variables relate to the company for which the strategy is decided as well as to the other companies holding a similar patent portfolio (e.g. all companies holding a DRM patent portfolio). The importance of the patents owned can be deduced from the strength of the patent protection on a technology and the importance of this technology to its field. In research on patent valuation three methods are used determine a patent's importance [Lanjouw et al, 1996] [Hall, 2000].

The first option is to count the number of times a patent is cited in other patents. A high number of citations indicates an important patent. A second option is to look at the number of times a patent has been renewed. Patents will likely not be renewed if they are of no value to their owner. The third option is to count the number of countries an innovation is patented. Important inventions will be patented in several countries and specifically those that are most important (e.g. the US and certain European countries).

In this specific case study it is not possible to calculate a numerical indication of a patent's strength using one or more of these three options. The technology is too new and therefore severely limits the use of citations[18] and excludes the use of renewal data. Comparing patents based on the countries for which patent protection has been sought is also not an option, as the search method used does not easily allow this[19]. Even though these patent valuation options are not used, it should still be possible to estimate whether the strength of a company's portfolio is below average, average or above average and place it in the model accordingly.

The willingness to license depends on the willingness of all relevant patent holders to license their patents, not just on the willingness to license of the company for which a strategy is decided. Of course if this company is unwilling to license a technology then this company should not follow a licensing strategy. A reason not to license can be, for example, that this technology will compete with another technology that this company prefers (e.g. because it is a money making opportunity). If however this company is willing to license, it has to estimate if others holding patents to the same technology are also willing to license. If these others are unwilling to license and their patents are important to this technology, it will likely be of no use to follow a licensing strategy.

---

[18] It does seem that InterTrust's patents are often cited, indicating a strong portfolio.

[19] The search method limits patents to one per family and as such, equivalent patents from different countries are removed.

Although predicting a company's licensing behavior can be difficult, it should be possible to estimate whether a company will not license at all, make it very difficult and expensive or make it easy (e.g. RAND) to get a license.

This model suggests a patent strategy based on the current portfolio. In some cases, however, a company will make such a decision not based on the patents it currently owns, but based on other factors such as the importance of the technology or the company's research efforts. The model should therefore not be seen as a definitive answer to the question of what patent strategy to follow, yet as a guiding advice.

The strategy choice model advises one of five strategy options, based on the importance of patents owned and the willingness to license. This is the model (figure 2.1) and an explanation of these strategy options:

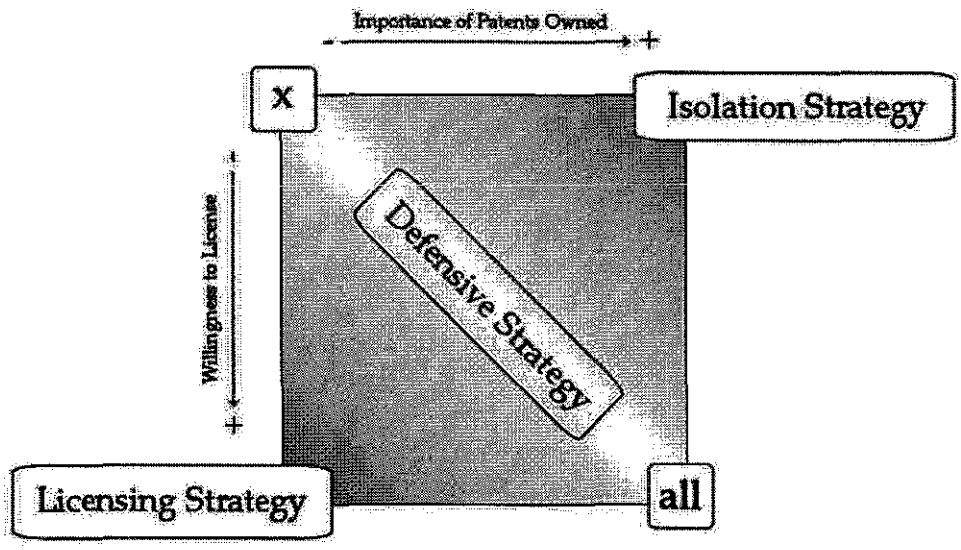


Figure 2.1: Patent Strategies

A **licensing strategy** is advised if a company's portfolio is of little importance and other patent holders are willing to license the technology. In order for the company to use the technology for its own products, it will have to purchases the necessary licenses. It is impossible to follow an isolation strategy in this situation as it is of no use to isolate the company based on technologies to which the patents do not provide sufficient protection (e.g. there are similar technologies available). Elements of a defensive strategy can be added to this licensing strategy to make sure the company can get licenses to all the patents it needs (e.g. using reciprocal licensing terms).

An **isolation strategy** is advised if a company holds important patents and is unwilling to license, for example because licensing the patents would not create sufficient revenues compared to being the only producer of a technology. Of course it is important in an isolation strategy that other companies do not hold patents that are essential to the technology or the product for which an isolation strategy is sought. If this is the case however and those other companies are not willing to license at reasonable terms a possible solution would be using elements of a defensive strategy. Leverage created by a defensive strategy (e.g. blocking these other companies' technologies) can be used to stimulate these other companies to license enabling the use of the isolation strategy.

A **defensive strategy** can be used in combination with both of the other strategies, but is specifically advised whenever there is too much uncertainty towards these other strategies. If the portfolio does not allow for an isolation strategy and there isn't enough willingness to license it is best to be defensive and keep both options open.

The "**X**" in the model portrays the situation where a company does not hold an important patent portfolio for a certain technology and those that do own an important portfolio are unwilling to license. If this company has no use for the technology that the model deals with, this does not necessarily create a problem. If the company does however want to use this technology it will have to either invent around the technology or license similar technologies. Another option is to create leverage by either expanding its portfolio with important patents or making the patents it owns more important (e.g. by pushing a standard to which these patents are essential). In a worst-case scenario strong defensive measures, perhaps non-patent related, could be used to create leverage.

The "**ALL**" in the model portrays the situation where a company holds a very important portfolio and is theoretically willing to license. All options are available in such a scenario and the strategy choice will depend on other factors, such as the factors that are discussed in §2.4. The situation of a company holding a strong portfolio yet also having a large willingness to license, is likely the result of this company wanting to stimulate the use of this technology (e.g. to increase licensing revenues) or the pursuance of a non-aggression strategy (e.g. licensing to all others in order to not give these other companies a reason to block the use of their patented technologies).

This model is used in chapter 6 as a guide for developing a strategy for Philips portfolio of DRM patents. As has been mentioned, there are many more factors that are relevant to the advised strategy. The influences the specific factors in this case have on the strategy choice are also detailed in that chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

3 Defining DRM

To better understand the ideas behind DRM, this chapter starts off with an introduction to the history of DRM. Next, an assessment is made of whether commonly used definitions of DRM render a viable option for defining what a DRM patent is in the context of this research. A new definition is presented, as the encountered definitions do not offer a practical demarcation for the technological fields to be included in this research. This new definition indicates that there are DRM enabling technologies, which themselves again need to be limited in the extent to which a patent covering these technologies will be considered a DRM patent. Furthermore two technologies that, like DRM, technically limit the interaction with content are discussed in this chapter to prevent any confusion over whether these technologies are or are not considered DRM technologies.

At the end of the chapter a classification scheme is presented that allows DRM patents to be classified to be compared.

Contents of this chapter:

3.1 DRM History

DRM originated at the XEROX Palo Alto Research Center (PARC), which at the time developed technologies around the "architecture of information". This research center was responsible for developments such as the WYSIWYG (What You See Is What You Get) text editor and Ethernet networks, both which have come into wide spread use. In 1996 Mark Stefik, an employee at XEROX Parc, introduced a new concept called 'Digital Property Rights' in his famous paper called 'Letting Loose the Light: Igniting Commerce in Electronic Publication' [Stefik, 1996]. It is this paper that is seen as the cradle of the concept of DRM. Many of the concepts introduced in this paper can be found in current DRM concepts. There are however also others who have come up with ideas that resemble DRM. The most important of these are Ted Nelson and Ryoichi Mori.

Ted Nelson, is the founder of Project Xanadu. Xanadu is an alternative hypertext system, used for inspiration by Tim Berners-Lee when he "founded" the World Wide Web [W3 org, a]. In the 1960's the concept of Transcopyright was introduced in Xanadu [Xanadu.com]. Essentially this concept allows for the management of rights over content. At the time it was introduced it was of little importance, but it seems to be in further development now that DRM has become a "hot issue".

Ryoichi Mori devised the Software Service System, now commonly known as superdistribution [Mori and Tashiro, 1987]. Superdistribution allows the free distribution of software, because the software is protected from modifications and modes of usage not authorized by its vendor. Superdistribution was originally aimed at distributing software, not video, audio or other types of content. The concept of attaching usage rights to the software does however resemble the concept of DRM. In fact the term superdistribution is now often used in combination with DRM. Its meaning has changed a little though, as it now denotes the concept of having users distribute all types of content amongst each other, while payment is still needed for a user to actually interact with the content.

The history behind the concept of DRM shows that this technology was originally aimed at managing the distribution to computer systems of software and later digital publications. Today, the scope of possible uses for DRM has greatly expanded and includes all kinds of content (e.g. audio and video) and all kinds of systems (e.g. consumer electronics). The next sections will show this as it discusses definitions of DRM and technologies used in DRM systems.

3.2 DRM Definitions

3.2.1 Commonly Used Definitions

In this section some examples of definitions of DRM that are commonly used are given, together with an indication of why these definitions do not suffice in demarcating what patents should be considered part of a company's DRM patent portfolio

In a presentation held for W3C (the consortium that developed Internet standards such as HTML) DRM was defined as involving *"the description, identification, trading, protection, monitoring and tracking of all forms of rights usage over both tangible and intangible assets - both in physical and digital form - including management of Rights Holders relationships"* [W3.org, b].

This definition lists a number of functions of a DRM system, but is too broad in its scope, as it does not limit these functions based on the technologies used to implement them. To illustrate the broadness of this definition we take a tangible asset in physical form, such as a book, and consider how for this object (allowed) rights usage would be described. A copyright notice in the cover accompanied by a warning that copying is not allowed without the publisher's permission, would be covered by this definition.

InterTrust, which owns many important patents on DRM, defines DRM as: *"the umbrella term for new business trust assurance processes designed to unleash the tremendous capabilities of the Internet. DRM technology provides tools to enable these new processes"* [InterTrust.com, a].

This definition describes a goal of DRM technologies, but gives no information on how DRM technologies reach this goal It also seems to limit DRM to Internet related technologies.

Microsoft defines DRM as *"a set of technologies content owners can use to protect their copyrights and stay in closer contact with their customers. In most instances, DRM is a system that encrypts digital media content and limits access to only those people who have acquired a proper license to play the content"* [Microsoft.com, a].

This definition describes why a DRM system would be used and gives an example of such a system. Like the previous examples, this definition does not give a clear indication of what would be considered DRM technologies.

3.2.2 *Definition for This Research*

As the definitions in the preceding section (§3.1.1) indicate, commonly used definitions do not present a viable option for defining DRM in the context of this research. In order to demarcate the fields of technology that can be covered by DRM patents, the phrase "Digital Rights Management" is parsed and its constituting elements are analyzed (see figure 3.1):

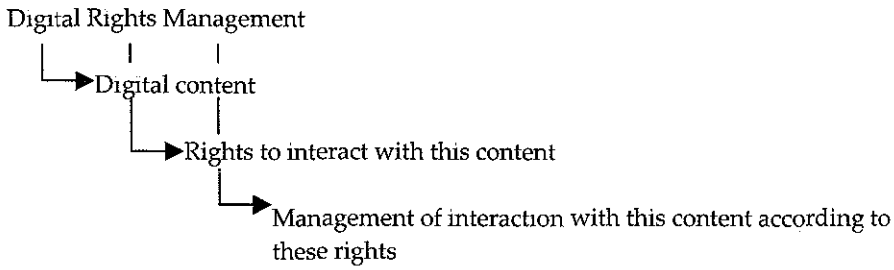


Figure 3.1: *Parsing Digital Rights Management*

According to this analysis, DRM patents are patents on managing interaction with digital content[20] according to interaction[21] rights. The definition proposed in this report is therefore: *'A DRM patent is a patent on a technology or the use of a technology for managing interaction with digital content according to interaction rights'.*

Both technology and the use of technology are mentioned, as a patent that should be considered DRM could cover both. As an example consider the following:

- A patent that claims a method of managing interaction with digital content according to interaction rights, such as a business method patent that claims a method of doing business by providing rights to interact with content in some way, is clearly a DRM patent. It covers the use of a technology, namely an applied business method that is covered by the definition given[22].

---

[20] The "digital" in DRM is believed by some to refer to the management of rights instead of the digital nature of the content. As DRM technologies can be found in the digital domain, both interpretations deal with similar technologies. However, not limiting the definition to digital content makes this definition much too broad In this section we try to limit the scope of the technologies that are considered DRM in order to create a guideline of what patents to include in this research. Therefore, it is prudent to choose a narrow definition.

[21] The phrase interaction is used here to express a multitude of actions that can be taken with content, such as playing (rendering) content, copying content, distributing content, etc.

[22] Such business method patents will usually mention the technologies used to implement the method, even if it is merely to attain the desired technicality of the invention that is needed for the patent to be granted. Therefore even for these types of patents it is necessary to list which technologies can be used to manage interaction with content according to interaction rights.

- A patent that claims the use of a technology to manage interaction with digital content according to interaction rights, such as a patent on the use of watermarking to embed rights into content, is also clearly a DRM patent. In this patent the innovative step will likely not be in the way interaction rights are specified or handled, but in the use of a certain technology to embed these rights.

The technologies that can be used in DRM can be seen as DRM enabling technologies. To indicate which technologies are DRM enabling technologies and to limit the scope to which the use of such a technology can be considered DRM, a short discussion on each technology is presented in the next section (§3.2).

3.3 DRM Enabling Technologies

This section covers DRM enabling technologies and their relation to DRM. For each enabling technology the extent to which a patent on the use of that technology is considered a DRM patent is discussed. To place the enabling technologies in a coherent perspective, a very general model of a DRM system is presented (see Figure 3.2). Each enabling technology discussed in this section can be used for a specific function in this model.

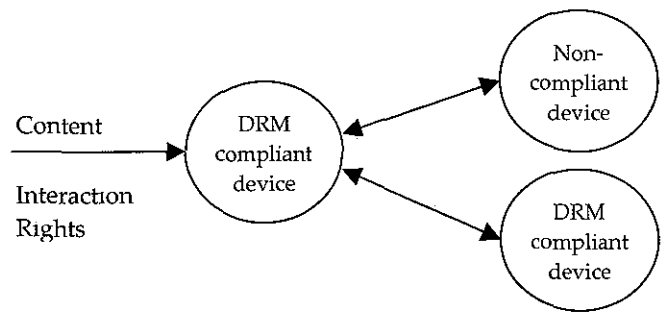


Figure 3.2: *General model of a DRM system*

In this model there are two types of devices: DRM compliant devices and non-compliant devices. A DRM compliant device is a device that interacts with content according to the interaction rights for that content. Non-compliant devices are all devices (that interact with content) that are not DRM compliant. A DRM compliant device receives content and interaction rights, not necessarily as one item or necessarily from the same source. This DRM compliant device can also communicate with other devices, both DRM compliant devices and non-compliant devices.

The functions present in this model are:

- Content management through content access protection: The compliant device receives content and the interaction rights for this content. Only compliant devices are able to interact with the content. Encryption, for example, can be used to limit access to content to DRM compliant devices (see § 3.2.1).
  There is an overlap between content access protection technologies and two other distinct fields of technology, namely Conditional Access technology and (certain) copy protection technologies. These two types of technologies are therefore discussed in §3.3.
- Content management through content authentication: The compliant device can check whether a non-compliant device has altered the content or the interaction rights For content that does not have rights associated with it, the device can detect whether this is licit content (e.g. legacy content and home-movies) or illicit content (e.g. illegal copies). Watermarking, for example, can be used to embed rights into content to prevent alteration (see §3.2.2).
- Device (compliance) management: A DRM compliant device can communicate with other devices. It is able to determine whether another device is DRM compliant or not and can securely exchange content with other DRM devices, in order to prevent the content from being 'tapped' during exchange. Certificates, for example, can be used to identify devices as being DRM compliant (see §3.2.6).
- Rights management: DRM compliant devices can obtain rights, create rights, alter rights, trade rights, etc. In principle all patents on these rights management methods, devices, etc are DRM patents (see §3.2.4).

An overview of the functions in a DRM system and some of the main technologies used for each function are depicted in Figure 3.3:

Content access protection	Cryptography
Content authentication	Watermarking Fingerprinting
Device compliance management	Trusted systems Digital signatures and certificates
Rights management	Rights (expression) languages

Figure 3.3: Functions and technologies of a DRM system

In the following sections these technologies will be explained in more detail. In the section on overlap with existing technologies, some more technologies will be introduced. For each enabling technology a quick overview of what constitutes a DRM patent and what does not, is included. The '–' sign indicates non DRM patents and the '+' sign indicates DRM patents.

3.3.1 *Cryptography*

Cryptography covers the methods of rendering information unintelligible (encrypting) and subsequently restoring this encrypted information to intelligible form (decrypting). In DRM cryptography is used during distribution or storage of content to render this content (or other data) useless to devices that do not have access to the decryption key. Usually a fast symmetric encryption algorithm is used to scramble the content and the key that this symmetric algorithm yields is encrypted using a slow asymmetric encryption algorithm. This has the advantage that it's fast (the slow algorithm is only used to encrypt the relatively small key) and secure (the key is asymmetrically encrypted which enables secure distribution).

There are uses of cryptography in DRM other than the scrambling of content. Cryptography is also used in identification schemes, for example. These uses are explained in further detail in section §3.4.1 and further.

- Patents on (implementations of) cryptographic algorithms are not DRM patents
+ Patents on the use of cryptography to encrypt content and interaction rights in order to prevent non-compliant devices access to this content or these interaction rights, are DRM patents.

3.3.2 *Watermarking*

Watermarking is used in DRM to embed information in content. The strength in resisting modification of the content these watermarking technologies offer differs. Some watermarks are better adapted to changes in the content, such as compression or resizing of video, than others. Often watermark technologies are therefore classified as robust, semi-fragile and fragile. A (semi-) fragile watermark is a mark that is (highly) sensitive to modification of the content and therefore used to detect (minor) changes of the content. A robust watermark has been designed to be difficult to remove and is used to permanently embed data in it. This data can cover interaction rights or content identifying information for example. To safeguard the watermark from being altered the watermarking algorithm (or the key used in it) is kept secret.

- Patents on (implementations of) watermarking algorithms are not DRM patents.
+ Patents on the use of watermarking to:
  - embed and retrieve information that is used to identify content as having interaction rights,
  - embed and retrieve interaction rights directly and
  - represent interaction rights

  are DRM patents.

3.3.3 *Fingerprinting*

Fingerprinting is a technology that computes a data identifier. In general, a one-way cryptographic hash is used, which is a mathematical function that takes data as input and produces as output a string of a fixed length. This output string is the fingerprint that will be the same every time the hash function is performed on the same data.

Most hash functions will give a dramatically different output, even if the input changes just a little. This makes these fingerprints ideal to detect changes when comparing data, but difficult to work with when identifying data. To illustrate this, consider that a hash function will return a completely different fingerprint for the compressed version of a song (e.g. a MP3 file) and the uncompressed version of that same song (e.g. CD). Therefore to allow identification of music, video or other data that has been compressed or altered, hash functions are needed that return fingerprints that can be related to the fingerprint of the uncompressed or unaltered data. These hash functions are called robust hash functions and these return similar fingerprints for similar data[23] [Haitsma et al, 2001].

A special use of hash function is the use for cryptographic tickets These are the digital equivalent of a paper ticket that is punctured to show it has been used. In DRM such tickets can be used, for instance, to indicate how many times content can be played. After each play the ticket is changed, making it a type of counter.

- Patents on (implementations of) fingerprinting methods, hash algorithms and such are not DRM patents
+ Patents on the use of fingerprinting methods, hash algorithms and such are DRM patents when used
  - to check whether content or interaction rights have been altered,
  - to identify a relation between content and interaction rights,
  - to identify devices as being DRM compliant or non-compliant

In general all patents on uses of fingerprinting methods, hash algorithms and such to identify data (e.g. content or interaction rights) for managing interaction with content according to interaction rights are DRM patents. A specific category of DRM patents covers the use of cryptographic tickets to manage interaction with content.

3.3.4 *Rights (Expression) Languages*

A rights (expression) language is used to communicate what interactions are or aren't allowed with content. Such a language consists, like human language, of grammar (structure) and vocabulary (expressions). These languages vary in complexity and human readability. The simplest variation is a bit-pattern where each bit expresses a certain state (e.g. never copy, play once). More complex variations use languages that are similar to human language.

---

[23] Such robust hash functions are in general specific for the type of data they are used on, such as music or video. Similar data could then be a song in a MP3 file and the same song on CD.

Some examples of commonly encountered rights languages are discussed here, as specifying what interactions with content are or aren't allowed is the core of DRM.

- MPEG Rights Expression Language (MPEG REL) and MPEG Rights Data Dictionary (MPEG RDD): The Moving Picture Expert Group (MPEG) has created REL and RDD as a part of the development of the MPEG-21 standard. This standard defines a multimedia framework that includes intellectual property management and protection. The REL (grammar) and RDD (vocabulary) standards together provide for machine-readable expression of interaction rights.
- Copy Control Information (CCI): In general CCI refers to a 2 bit long pattern that covers 4 copy related interaction rights: copy not controlled, copy once, copy no more and copy never. Other, more complex, implementations of copy control information are possible.
- Digital Property Rights Language (DPRL) or eXtensible Rights Markup Language (XRML): Mark Stefik of Xerox (see §3.1) developed DPRL as a machine-readable language that could be used to define access rules and procedures, for use in a trusted environment. The second version of DPRL is XML-based making it interoperable with other emerging standards and enabling it to adapt to changing needs. The language was renamed XRML to indicate its use of XML, when Xerox and Microsoft jointly launched the company ContentGuard to further develop the language [Whatis.com].

– Solutions to (practical) problems encountered in the field of rights (expression)languages. These are likely highly related to the choice of what language to use in a DRM system.

\+ All patents on (the use of) such languages are important in this research and therefore all of these patents are, in principle, DRM patents. However, it is unlikely that (elements) of such languages can be patented. A rights (expression) language as such can not be patented for instance.

3.3.5 *Trusted Systems*

Technologies used in trusted systems (also referred to as trusted computing, trusted services, controlled environments and such) are used in DRM to limit interaction with content according to the interaction rights. A trusted system is usually built around trusted hardware and a core of trusted software, together often called the trusted computing base. This base can then allow other software and hardware to enter the trusted environment. In DRM this principle can be used in determining which systems are allowed to receive unencrypted content or the keys needed for decryption.

Another set of technologies that is used with trusted systems prevents tampering with hardware or software. Such tamper-proof technologies prevent access to keys, unencrypted content or interaction rights. These technologies range from software protection measures that prevent reverse engineering to chip manufacturing methods that hinder useful data to be gathered with an electron microscope.

- Patents on trusted systems or tamperproof technologies are not DRM patents. In general every DRM compliant device is a trusted system and therefore patents mentioning merely that the system or architecture claimed can be used for DRM compliant devices, does not indicate that it is a DRM patent.
+ Patents on the use of trusted systems and related technologies to limit the exchange of content from compliant devices to other devices, including methods of determining whether devices are compliant, are DRM patents.

3.3.6 *Digital Signatures and Certificates*

Digital Signatures use asymmetric cryptography to identify and authenticate digital information. A digital signature is a piece of data (e.g. a fingerprint) that identifies digital information that has been encrypted. The identifying data is encrypted using a private key and decrypted using the matching public key. Anyone that has the public key can decrypt the signature this way and knows that only the person / device that has the matching private key could have encrypted it.

There are two requirements for the identification and authentication to be correct. First of all the private key must be kept secret, otherwise the digital information could have come from anyone that knows the key. The second requirement is that both the relation between the public and the private key as well as the relation between the private key and the sender of the digital data must be established. If someone sends a public key, you need to be able to trust that the person sending it really is who he says he is and that the public key that is send is the match for his private key.

This is where digital certificates prove their usefulness, as they certify electronic identities. A certificate for a certain identity is this person's public key encrypted using the private key of the certificate's sender. If the receiver trusts the sender of the certificate, then the receiver trusts that the public key he will use to decrypt a digital signature belongs to the specified identity. In general these certificates are retrieved from a Trusted Third Party also known as a Certificate Authority (CA). This is an entity that is trusted by multiple parties. Such an entity can require some sort of identification to be provided before it will create a certificate.

When several CA's are combined an infrastructure is created; this is referred to as a 'Public Key Infrastructure (PKI)'. A PKI is essentially the framework that issues, maintains and revokes public key certificates. Another term that is often used in digital signature and digital certificate technologies is 'key management'. Key management covers the control of generating, storing, protecting, transferring and destroying keys used in cryptography.

- Patents on (implementations of) digital signatures, digital certificates and such, are not DRM patents.
+ Patents on the use of digital signatures, digital certificates, key management and such, to identify, certify and authenticate DRM compliant devices are DRM patents This includes methods of revoking keys to manage interaction with digital content according to interaction rights (e.g. keys that give devices access to content and keys that authenticate interaction rights).

3.4 Overlap with Existing Technologies

Copy protection technologies and Conditional Access (CA) technology, like DRM, manage interaction rights to content, but only to a limited extent. Copy protection can limit copying of content and CA can limit access to content. To prevent any confusion as to whether patents on these technologies are DRM patents, these technologies are reviewed.

3.4.1 Copy Protection

Copy protection technologies deter piracy by limiting the possibilities of copying content. Certain, but not all of these technologies are relevant to this research. A distinction is made between:

1. Technologies that prevent copying that use unintentional design features of copying equipment (these are not based on expressing interaction rights).
2. Technologies that prevent copying that are based on expressing interaction rights.
3. Technologies that can be used to limit access to certain devices (which in general do not enable free and unlimited copying of content).

Copy protection using unintentional design features

These are copy protection technologies that prevent copying that are *not* based on expressing interaction rights. In general these technologies exploit features of the copying apparatus that were not intended by design to be used in a copy protection scheme. Copy apparatus can therefore often be redesigned to allow copying. These copy protection technologies are not considered DRM, as no rights are involved

Examples of such technologies which are not considered DRM are:

- Using an Illegal Table of Content (TOC) on a CD, placing data on a CD outside the defined reading/writing area (overburning), putting physical errors on a CD and putting faulty error correction codes on a CD or otherwise updating the standard for the compact disc. All of these technologies prevent direct copies to be made of a CD. They use design features of CD readers and writers to generate read or write errors which abort the copying process. Redesign of CD readers, writers and software have made these technologies useless in most cases[24].
- Macrovision's Analogue Protection System (APS). This system is based on altering the video signal in such a way that a videocassette recorder (VCR) will introduce faulty picture information in the copy, rendering it worthless. Circumventing this measure is technically possible by redesign of the VCR or by adding a device that filters the signal disturbances. Redesign of the VCR is difficult as the VHS standard includes this design feature[25]. Using filtering devices is legally difficult, as Macrovision has patented most of such filtering technologies.

Copy protection using interaction rights

Copy protection technologies that prevent copying based on expressing interaction rights, usually allow different interaction rights (copy once, never copy etc.) to be distinguished. In general these technologies require specific intentional design features to be present in the copying and/or the reading device. As these technologies use interaction rights to express how content can be interacted with, these are clearly DRM technologies.

Examples of such technologies which are considered DRM are Copy Generation Management System[26] (CGMS) and Serial Copy Management System (SCMS). Both technologies add a signal to the content that expresses whether copying is allowed, not allowed or only allowed for first generation copies. A compliant system will pick up this signal and limit copying accordingly.

---

[24] As redesign limits the usefulness of these copy protection technologies, new technologies are developed. Some audio CD's are currently protected by key2audio [Key2Audio.com], cactus data shield [Midbartech.com] and other technologies. All of these again seem to rely on exploiting features of CD readers or writers that were not intended to prevent copying. Redesign is not predictable, therefore some technologies might prove to deliver long term copy protection value.

[25] Although this was originally not an intended design feature, changes to the VHS standard seem to have made the susceptibility of VCRs to Macrovision copy protection part of the VHS specifications.

[26] Sometimes also referred to as Copy Guard Management System. There are both analog (CGMAS-A) and digital (CGMS-D) versions of CGMS.

Copy protection by limiting access

Copy protection technologies used to limit access to certain devices, can be a part of a DRM system. These technologies can be used to limit access to content to DRM compliant devices or to authenticate content. These technologies are DRM technologies.

Examples of such technologies which are considered DRM are:

- Content Protection for Recordable Media (CPRM) and Content Protection for Prerecorded Media (CPPM)[27]. Both use encryption of content and unique keys for both content readers (e.g. DVD player) and medium (e.g. DVD-R). The key on the medium is placed there during the manufacturing process and is irreplaceable. The content key can only be decrypted if both the medium and reader key is known. As a copy will have a different media key than the original, a copy can't be accessed Legal copies can be made by changing the content key. Only a compliant device should be able to do this and such a device will only do this if the rights to copy aren't violated this way.
- Physically marking the content medium (e.g. placing a wobble on a CD). These technologies are based on the impossibility of copying the mark using consumer equipment (i.e. redesign of the consumer equipment is virtually impossible due to high costs). The content will only be played when the mark is present. Redesign is often not viable, as marking the media requires expensive equipment. In DRM this can be used to authenticate content based on the physical carrier (e.g. by placing a watermark in the content with the fingerprint of wobbles in the CD the content is supplied on).

3.4.2 *Conditional Access*

Conditional Access (CA) systems are most often used with cable and satellite television, but other uses are possible These CA systems use encryption to protect content during transmission, allowing access to the content only to devices that have been authorized to do so (e.g. a set-top-box). Although CA systems can be seen as a predecessor to DRM systems, they only allow for control of access[28].

Furthermore, Philips' patents on CA technologies are already identified within Philips IP&S. There is no need for these technologies to be included in this research and therefore CA technologies will be excluded from our definition of DRM. CA technologies can however be used in conjunction with DRM technologies and patents could cover DRM and CA technologies at the same time in which case they should be labeled as both CA and DRM.

---

[27] CPRM and CPPM also use revocation lists to prevent hacked devices from being used. This is however not of importance in this section.

[28] Technically this could be used to protect copying and such, by allowing access to free-to-copy content to all devices and access to copy protected content only to devices that aren't capable of copying. In practice such schemes are not used

3.5 DRM Patent Classification Scheme

Philips uses a company-wide patent search system that categorizes patents based on the product division to which they are relevant and based on the technology a patent covers. The research assignment that was performed for Philips included the creation of a classification scheme for DRM patents that could be integrated in the existing classification. Within the context of this research it is not necessary to include this detailed scheme completely. Instead a simplified version is presented here, which can be used to compare different companies' patent portfolios at a later stage in this paper (§5.3).

The scheme is based on the model presented in §3.3 and includes four main classes, each with several subclasses (see figure 3.4):

1. Content management - this class covers securing content, which consists of limiting access to content to compliant devices, authentication content to certify it is not illicit, converting content to use it or export it to another device and finally it also includes binding rights to content. The latter covers methods of creating a secure relation between content and the rights that pertain to this content.

2. Device (compliance) management - this class covers the management of DRM devices and creating a "world" of compliant devices. The successive steps in compliance management are deploying devices, identifying and authorizing to other devices and exchanging data between devices. There are two more important aspects to device management, which are creating interoperability between different types of devices and revoking devices that should no longer be trusted.

3. Rights management - this class covers all methods of handling rights of which the most basic elements are: a rights model that specifies which rights and options exist, methods to obtain these rights (e.g. peer-to-peer or through a specific server), methods to transmit these rights to devices or users (e.g. embedding rights in the content or distributing them in a physical way) and finally the processing of rights by devices (e.g. calculating whether or not to allow the use of content based on the attached rights).

4. Related aspects - this class covers aspects that are closely related to DRM, but are not directly related to content, devices or rights. This class has five subclasses, but can also be assigned without the specification of a subclass. The subclasses cover the circumvention of content protection, the monitoring and tracking of content (usage), privacy enhancing aspects of DRM systems, DRM system architectures and DRM business models (e.g. methods of selling licenses).

Digital Rights Management Patent Classification	
Main Class	Sub Class
1. Content management	1. Content access protection 2. Content authentication 3 Content conversion (incl. export) 4. Binding rights to content
2. Device (compliance) management	1. Deployment 2. Identification (and authorization) 3. Data exchange (incl. key exchange) 4. Interoperability 5. Revocation
3. Rights management	1. Rights modeling 2. Obtaining rights 3. Transmitting rights 4. Processing rights
4. Related aspects	1. Circumvention technologies 2. Monitoring and tracking 3. Privacy enhancing aspects 4. System architecture 5. Business models

Figure 3 4: DRM patent classification scheme

Most of the subclasses in each class can use one or more of the following technologies. The most important of these are:

1. Using watermarks
2. Using tickets
3. Using fingerprints
4. Using certificates
5. Using encryption
6. Using wobbles

9. Using complete data sets (a technology only used by Philips)

These can optionally be used as a sub-sub-class. however not every patent will specify one of these technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

4 Searching for patents

In this chapter, a method is presented to create a search for (DRM) patents. The method consists of finding keywords that relate to DRM and then limiting the results of the search based on patent classifications.

At the end of the chapter the search results are discussed.

Contents of this chapter.

4.1 Introduction

There are many reasons why patent searches are conducted and therefore there are many different types of searches. These are some examples:

- Patentability searches (also known as novelty searches or prior art searches) are conducted to find out if an innovation can be patented;
- State of the art searches try to provide an overview of a certain technology;
- Infringement searches are conducted to find out if a product infringes a patent;
- Validity searches are done to find out if a patent is valid;
- Competitive intelligence searches are conducted to find out which companies hold patents in a certain field of technology.

These searches are conducted in online patent databases. For this research three of such databases are used[29]. These databases allow searches to be conducted based on[30]: keywords, patent classifications, inventor names, assignee of the patent (i.e. the company that owns the patent) and some less-relevant search items[31].

In this research a search is conducted to find patents on DRM technologies owned by Philips[32] and others. The search method used consists of three steps (see Figure 4.1), which can be outlined as explained on the next page.

---

[29] The patent databases used in this research are MicroPatent, Pluspat in Questel/Orbit and EspaceNet. The first is used to search using keywords, the second is used to limit the scope of the search to certain classes and the third is used to supplement data manually when data on a certain patent is missing in one of the other databases or needs to be verified. The choice for the two main patent databases Micropatent and Pluspat in Questel/Orbit, limits the completeness of the list of patents in two ways. First, only published applications and granted patents can be found in these databases. This is however the case for any of the publicly available[29] patent databases. Only for the patents assigned to Philips would it have been possible to search the unpublished applications Secondly the databases used cover only US / WO / EP / GB / DE and JP patents. Again, almost all patent databases know similar limitations and therefore there is little choice in this matter. It would be possible to use several national patent databases besides Micropatent and Pluspat in Questel/Orbit, but this would negate the main benefit of using these two selected patent databases, namely the timesaving effect.

[30] Although not every database allows for the exact same methods (e.g. databases usually use different types of classifications).

[31] The less relevant methods of finding patents in a database are either aimed at finding a specific patent of which some information is known (e.g. publication number) or are for another reason of limited use in this research. Searching based on a publication date is for instance, of little relevance here.

[32] Patents assigned to Philips can be listed in a patent database as having one of several assignees, such as "Philips Electronics" and "Koninklijke Philips". Using "Philips" and "Cryptoworks" as entries for these fields will return all patents owned by Philips that could be relevant to the search. Searching for "Philips" as assignee will return patents assigned to "Philips Electronics", "Koninklijke Philips" and all others that contain the word Philips. "Cryptoworks" is the only name used in this field by Philips that does not contain the word "Philips". A manual review of the results prevents patents from being included that are owned by other companies than Philips that have a name that includes the word "Philips".

1. Keywords are used to create a query to find relevant patents[33] and as such these keywords determine the completeness of the results (i.e. whether all DRM patents are included in the results). If a patent contains no keywords that are in the query that is used in the search, it will not be found. The soundness of the results (i.e. whether all patents that are found are DRM patents) is also determined to some extent by the keywords used. If irrelevant keywords are used more irrelevant patents will turn up in the results.

2. Patent classifications are used to limit the scope of the search and therefore can increase the soundness of the results. By searching only in relevant classes of patents (e.g. by not searching chemical patents), irrelevant patents can be 'filtered' out of the results obtained by searching using keywords. However, a choice for the wrong set of classes to filter patents on can decrease soundness.

3. By searching using the names of people who have done research on DRM (related) technologies for Philips, the results of the previous steps can be verified for the Philips DRM patents. If all of the relevant patents that are found using the names of inventors are also in the results of the query, it is very likely that the results of the query are complete. Although this method can only be used for the Philips DRM patents, the completeness of these Philips patents in the query can be seen as an indicator for the completeness of all DRM patents in the query.

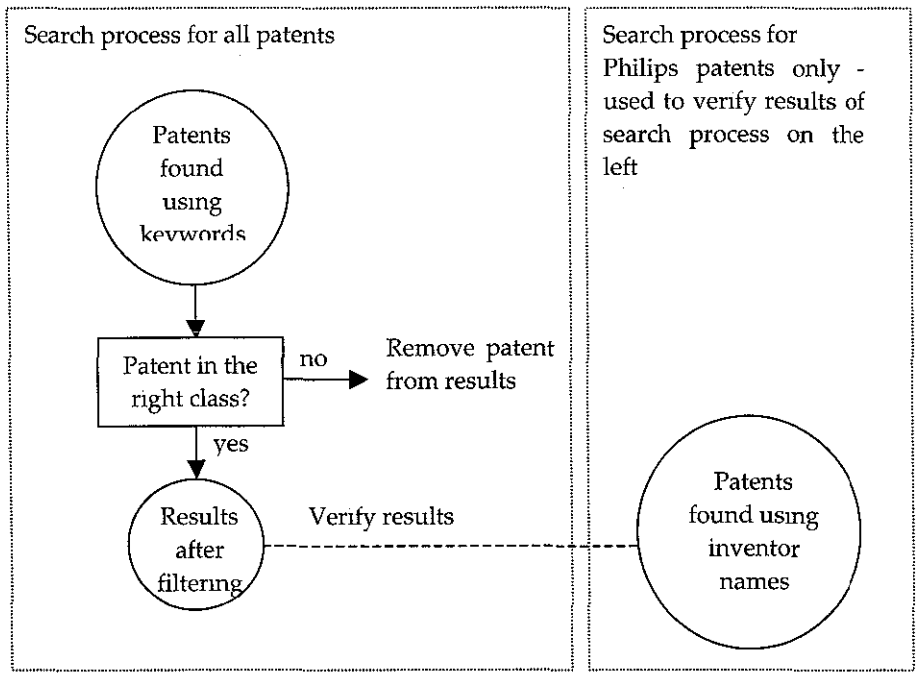


Figure 4.1: Search process

[33] Operators can be used to make such a search more specific, by combining words or phrases or by allowing some variation in a phrase. In this report a combination of keywords using operators, will be called a keyword (e.g. 'rights' and 'management' is a keyword, but 'rights AND management' -which searches for both words to appear in the same patent - is also called a keyword).

4.2 Searching Using Keywords

4.2.1 Finding Keywords

Prior to formulating any queries there are two questions that have to be answered. These are the questions of how to determine what keywords will be used and what part of the patent to search using these keywords. In determining what part of the patents will be searched for appearances of keywords, there are only limited options. Searching only the title or abstract of the patent is unlikely to return all relevant patents. Most patent titles and abstracts use more general descriptions than the descriptions used in the state-of-the art, the preferred embodiments, the claims and other parts of the patent. Therefore the complete patent will be searched, allowing relevant patents to be found that do not mention the keywords in the title or abstract[34].

Determining the keywords to use is not a part of the search process that can be dealt with prior to performing the actual search. During the search "hands-on-knowledge" gained, leads the way as to what keywords to use. Based on the definition and short review of the history of DRM as outlined in Chapter 3, the types of keywords found in figure 4.2 seem appropriate.

Keyword types	Examples of keywords
General names for DRM	Digital rights management, content rights management, super-distribution, etc.
Architectural elements	License server, content server, etc.
System elements	Distribution: secure distribution, etc. Trust: trusted client, etc. Language: rights language, etc. Management: intellectual property management, etc
DRM standards	Secure Digital Music Initiative, Digital Object Identifier, etc.
DRM "founders"	Mark Stefik, Ryoichi Mori, etc.
Enabling technologies	Watermarking, fingerprinting, etc
DRM functions	Protection of digital works, royalty payment, etc.
Related technologies	Copy protection, conditional access, etc.

Figure 4.2: Finding keywords

[34] It comes to mind that certain terms could be searched for in the full patent text and others in the title or abstract. The part of the patent (e.g. title) a keyword is found in can indicate the relevance of that keyword for the patent. A patent titled "Method for management of content usage rights" would very likely be specifically about a DRM technology, while the same phrase found in part of the complete text of a patent could just indicate a possible use. However, we have found that titles and abstract are often of very limited value in indicating the technology that is claimed, therefore we will not make our search needlessly more complicated by searching for different phrases in different parts of the patent.

Different manifestations of each phrase are used during the search. A search for "digital rights management" should, for instance, cover other terms denoting the same technology such as "electronic rights management". Choices as these are made during the search process and will not be discussed in this paper, but in the appendix (see Appendix A).

Another type of choice that is made during the actual search process, is how to combine these keywords using (boolean) operators. A search for all patents containing the words rights and management, will return patents that mention these each in a different context[35]. Therefore it is better is to search for patents mentioning "rights management" as one phrase or search for both words if they are no more than, for example, three words apart. Again these choices are not discussed in this paper, but in the appendix (see Appendix A).

The search using keywords consists of an iterative process of fine-tuning the query to return a set of DRM patents that is as complete as possible Irrelevant results can be filtered out, either using the patent classifications or manually. Therefore it is desirable to aim the query at complete results rather than limit completeness in return for greater soundness. The creation of the final search query takes place in several steps:

- Query 1 is formulated using several keywords that are strongly related to DRM Testing this query provides a first set of results, which can be reviewed to ensure the patents the query finds are really DRM patents (see §4.2.2).
- Adding additional keywords to the first query creates query 2. In this process, the results of Query 1 are used to give an indication whether a keyword should be added to Query 2 or not (see §4.2.3).
- Adding an additional number of keywords to Query 2 creates Query 3. This process does not use the method that is used for creating Query 2. Instead, the results of each keyword are reviewed and based on the number of relevant patents that are found, the keyword is either added to the query or dismissed. This process is continued until it becomes clear that no more relevant keywords can be found.

Query 3 is then used to find a list of DRM patents that is filtered using the classification of these patents (see §4.3).

---

[35] For example the following patent will be encountered upon such a search:
US patent US20020090268: MICROWAVE ENERGY APPLICATOR
"Dwindling ground water resources, water allocation *rights* disputes, and water pollution results in an inability to farm on land that would otherwise be productive but for the lack or uncertainty of water availability from planting through harvest. Government regulations, in an attempt to correct current problems, often only further hobble the farmer Land use and growth *management* laws effectively lock up potential farm lands."

4.2.2 *Query 1*

In order to compose Query 1, which has to return results relevant to DRM (for reasons explained in § 4.2.3), a limited set of keywords likely to be used in patents on DRM technology are tested. These keywords and the analyses of the outcomes of searches based on these keywords are discussed to give an example of the method that is used both here and in other parts of the search. The following is a list of these keywords and the results of the queries based on these keywords[36] (the exact queries and results can be found in Appendix A):

Keyword	Results of a search using this keyword
Rights management	Good results: many of the patents seem to deal with DRM. Prefixing the phrase with "digital", "electronic" or "content" leaves out to many relevant results.
Content management	Bad results: very few patents deal with DRM.
Product management	Bad results: most patents deal with physical products. Prefixing the phrase with "electronic" or "digital" leaves only one patent and that patent does not deal with DRM.
DRM	Bad results: DRM is used as an abbreviation for many other technologies. Very few results deal with DRM and those that do also mention "digital rights management".
License server	Bad results: most patents deal with software licenses.
Content server	Bad results: very few patents deal with DRM.
Royalty payment	Bad results: many of the patents cover methods of paying royalties. There are some DRM patents in the results, but these are also in the results of the "rights management" query.
Superdistribution	Good results: many of the patents seem to deal with DRM.

Figure 4.3: Reviewing the results of keywords

Based on these findings, Query 1 is chosen to include only keywords for "rights management" and "superdistribution". Some of the keywords that are not selected for Query 1 will be tried again in Query 2 with different variations.

[36] The queries based on these keywords are designed to leave room for some variation. The search for "rights management" is formulated as "right*1 management". This will return patents with occurrences of "rights management" as well as "right management".

4.2.3 *Query 2*

As it is impossible to know beforehand exactly which words are used in patents to describe DRM technologies, finding the right keywords is a process of trial-and-error. However, this does not mean that it is an unscientific process consisting merely of guessing keywords. The method used in this search process is to use the simple Query 1, which returns results that are representative for DRM patents, and compare these results to the results of searches using new keywords.

For each search using a new keyword, the overlap between the results of such a new search and Query 1 are calculated. If the new search returns many of the same patents as Query 1, then the keyword used for this new search is likely used often in DRM patents. This is illustrated in Figure 4.4 (see below).

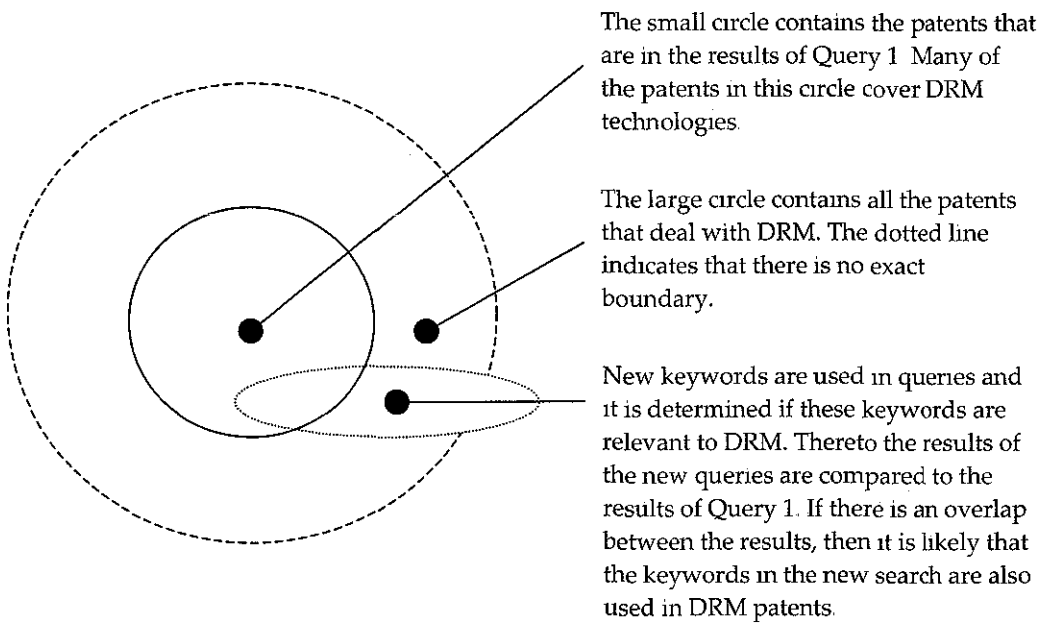


Figure 4.4: Process of finding new keywords

Although a large overlap between the results of a search using a new keyword and the results of Query 1 can indicate that the keyword is relevant and should be included in Query 2, it could also indicate one of the following:

- The keyword is very general. As it is used in many patents in general it is used in many DRM patents as well. This could be indicated by a fairly large overlap between the results of Query 1 and the results of the search using the new keyword, in combination with a large set of results for the new keyword in general when compared to the results of Query 1.
- The keyword is relevant to a DRM related technology and the patents in the results of the search using the new keyword are patents on this related technology not all dealing specifically with DRM

The results of each new search are therefore reviewed and particular attention is paid to the patents that are in the new query, but not in Query 1. Random manual review of titles and abstracts of some of the patents in the result set is performed to determine if these are DRM patents. In case these are DRM patents, then the keywords used to find these patents should be used in the search for DRM patents, hence these keywords are appended to Query 1 to form Query 2.

The graphical representation of the overlap between the results of three searches using new keywords and the results of Query 1, indicate in this example that the second query ("rights protection") seems relevant (see Figure 4.5).

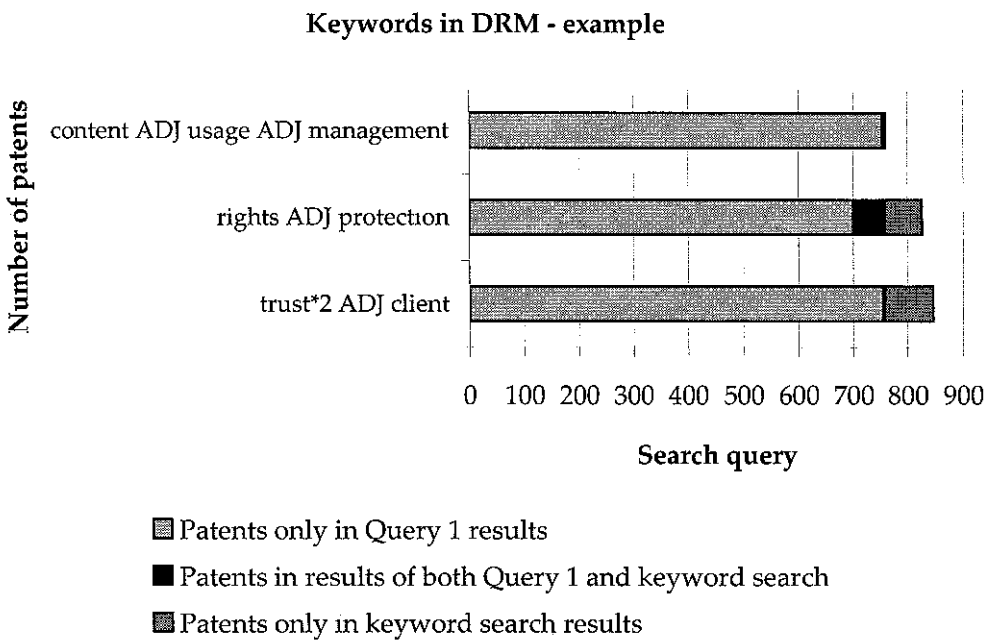


Figure 4.5: Example of trying keywords to find which are relevant

The second query shares about as many results with Query 1 as it returns new ones. The first query returns no new queries and has only minor overlap with Query 1. The third query does return new results, but has no overlap with Query 1. A manual review of the results confirms that the new keywords of the second search are relevant and the new keywords of the first and third search are not.

After manually reviewing the keywords that seem relevant and some of the keywords that seem irrelevant as well (for purposes of verification of the method), a list of keywords is made that are important in searching for DRM patents. These keywords are then appended to Query 1, to form Query 2 (see Appendix A).

4.2.4 *Query 3*

A comparison of Query 1 to Query 2 shows that completeness has increased, but soundness has decreased. A rule of thumb used in many sciences is the 80-20 rule. In this context this rule indicates that 80% of the results are found in 20% of the time. Finding the other 20% of the results takes the other 80% of the time. Although in this context this rule of thumb is not well-founded by empirical research, it does seem to be true. At the very least the rule indicates that each step in this iterative search process will return fewer relevant results. Finding new keywords to append to Query 2 to form Query 3, will therefore be more difficult. The method used in the transition from Query 1 to Query 2, as explained in the preceding section §4.2.3, will therefore not be used here.

From Query 2 to Query 3, only manual reviews of the results are performed to determine the relevance of keywords to the search for DRM patents. The keywords used and the results of searches on these keywords are not discussed in this report, but can be found in the Appendix (see Appendix A).

Query 3 is the final query to be used in this search. The next step, filtering the results based on the classification of the patents, is performed only to increase soundness. DRM patents that are not in the results of Query 3, will therefore not be found in this search. The difficulty of finding more relevant search terms in the process of forming Query 3, is an indication that the results of Query 3 are nearing completeness. Full completeness can however never be claimed, as there is no complete list of DRM patents to verify the results of Query 3. If there were such a list, this search would not have been necessary in the first place.

It is therefore likely that the final query can still be optimized; yet this will be very time consuming. As DRM patents of other companies need only be found to determine a general patent strategy (i.e. not a patent strategy surrounding one invention) the results are deemed adequate to use Query 3 as the final query[37].

[37] For further research of the patent portfolio of a specific company other than Philips, it is recommended that such research should be preceded by an optimization of Query 3 to increase soundness of the results for that specific company.

4.3 Limiting the Search Using Patent Classifications

Patents are classified to allow for easy searching based primarily on the function of an invention, as patent offices need to find relevant patents when trying to determine the novelty of a new patent application. There are however also other uses of patent classifications. Companies can, for example, search for specific patents when determining what technology to use or what research to do. In this research the classifications are of use in searching for patents that deal with DRM technologies.

The very first patent classification systems were alphabetical lists of granted patents. France, for example, made a list of this kind in 1791. This type of list lost its usefulness as the number of patents grew. In the United States the patent office introduced a classification in 1872 that used classes based on the technological subject the invention dealt with [Wipo.int, a]. Soon other countries followed in introducing patent classifications.

Attempts were made to create an international classification, but the first attempts failed. The fact that these attempts were made since the end of the 19th century shows the need for such an international patent classification. In 1949 the first steps were taken in the creation of a European patent classification system. The use of this European classification was expanded when the "Strasbourg Agreement Concerning the International Patent Classification" entered into force in 1975 and made this classification the international patent classification (IPC) [Wipo.int, a].

There are four main patent classification systems in use today:

1. International Patent Classification;
2. European Classification;
3. US Patent Classification; and
4. Derwent Classification.

In this research two of these classifications are used, namely the International Patent Classification and the European Patent Classification. The Derwent classification is not used in this research, because it is not available in the patent databases that are used[38]. The US patent classification is not used as it is by far not as effective as a filtering mechanism as the combination of ECLA and IPC. This will be explained in more detail in the following sections, which introduce in more detail the classifications used.

[38] The Derwent classification is available in Quertel/Orbit, but not in the Pluspat database used in this research.

4.3.1 *Introduction to the International Patent Classification*

The International Patent Classification (IPC) has been used for over 25 years and is used by over 90 states today[39] [Wipo.org]. Almost every patent will therefore have an IPC class associated with it. The classes are based on the function of the invention and the classification is hierarchical. An example of the IPC classification of a patent demonstrates this. The ContentGuard patent entitled "System and method for protection of digital works" can be found in IPC class G06F 1/00 [Patent EP1146411]. This means it is in (see figure 4.6):

Section.	G	Physics
Class:	06	Computing; calculating; counting
Subclass:	F	Electric digital data processing
Main group:	1/00	Details not covered by other groups
Not in any subgroup		
	G06F 1/00	

Figure 4.6: Example of IPC patent classification

The ContentGuard patent used as an example here is not in any subgroup. If it were in a subgroup, then this would have been indicated as follows for example for subgroup 2 of main group 1: G06F 1/02. The hierarchy of subgroups is a little more complex than the hierarchy of the rest of the IPC classification. The hierarchical position of a sub group can't be determined by looking at the number of the subgroup alone, as it is determined by the number of dots in front of the title of the subgroup[40]. The following example (Figure 4.7) clarifies this:

1/00 Title of the group

1/02 . Subgroup title 1

1/04 .. Subgroup title 2

1/06 ... Subgroup title 3

1/08 . Subgroup title 4

1/10 . Subgroup title 5

1/12 .. Subgroup title 6

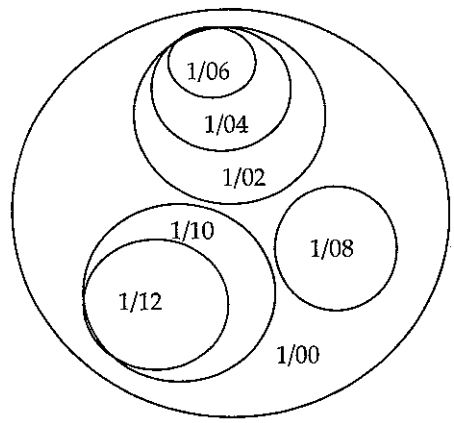


Figure 4.7. [Wipo int, a] The dots in front of the subgroup title indicate that it is a subgroup of the first group above it with one less dot (e.g. 1/12 is a subgroup of 1/10 which is a subgroup of 1/00)

[39] Although not all of these states have signed the IPC agreement.

[40] Which can be found in the classification which is available online

The current (seventh) edition consists of 8 sections, 120 classes, 628 subclasses and almost 69,000 groups [Wipo int, a]. The IPC is updated every 5 years, but patents are not reclassified. On a patent it is indicated which version of the IPC has been used in determining the class. To find a patent by searching a specific class, the IPC version is needed that was used at the time the patent was classified. To find a patent classified in 1997, for example, IPC version 6 is needed (used from 1-1-1995 until 31-12-1999) instead of the current version 7. As the changes between the previous and the new version of the IPC are denoted in the new classification, it is easy to find out if these changes are of importance to the query[41].

4.3.2 *Introduction to the European Classification*

The European Classification (ECLA) is the internal classification of the European Patent Office (EPO). This means that an ECLA classification will only be found on patents that have been processed by the EPO. Only a few patent databases offer the option of searching using the ECLA (e.g. Pluspat in Questel/Orbit and Esp@ceNet). The ECLA is an extension of the IPC classification. For example, the patent used in the previous example can be found in European classification G06F 1/00N7R2, which is a subclass of the IPC class it is in (G06F 1/00):

N – Protection against unauthorized activity relating to computers and software
7 – by manipulation of programs or processes
R – to restrict resource availability, e.g. access to programs or data
2 – by controlling access to software, e.g. licensing, vending or distribution

The ECLA can therefore be used to make a search more specific than by using 'just' the IPC. There are more differences between the IPC and ECLA [Epa.org]. One important difference is that the ECLA is changed whenever this becomes necessary and patents can be reclassified. Searching for very new technologies can therefore be easier in ECLA, yet older patents will still be classified according to the latest version of the ECLA classification. Another important difference is that in the ECLA all patents are classified within a particular technical field by the European patent examiner responsible for searches in that field. The ECLA is therefore a more coherent and consistent classification than the IPC which is determined by different patent offices throughout the world.

Finally, even though the ECLA is an extension to the IPC, a document that has been assigned an IPC classification could be assigned a different ECLA code, as examiners of the European Patent Office do not necessarily take an already assigned IPC code of a patent as their basis for the ECLA classification[42].

---

[41] There have been no changes between IPC's version 5, 6 and 7 that affect the selection of classes made in this research.

[42] For example, CRYPTOWORKS INC patent on a "DIGITAL PRODUCT RIGHTS MANAGEMENT TECHNIQUE" has IPC Classification H04L9/00 and EC Classifications: G07F7/00C, G06F1/00N7R2, G07F17/16, H04L29/06C6B. It does not have an EC classification based on its IPC classification [Patent WO 1998/42098].

4.3.3 *Determining the Classes Relevant to DRM*

In determining the classes that are relevant to DRM, two approaches are used. The first approach consists of a manual review of the IPC classification and subsequently the ECLA classification, to determine the relevant (main and sub) groups. In the second approach, known DRM patents are reviewed to determine which IPC and ECLA classification they've been assigned.

The first approach is illustrated in Figure 4.8 (see below). As the IPC classification is hierarchical, a manual review does not require every class, subclass and main and sub group to be reviewed. For the IPC for example only 2 of the 8 sections (G and H) can be assigned to DRM patents. This eliminates the necessity to review a large number of classes and therefore subclasses and groups as well.

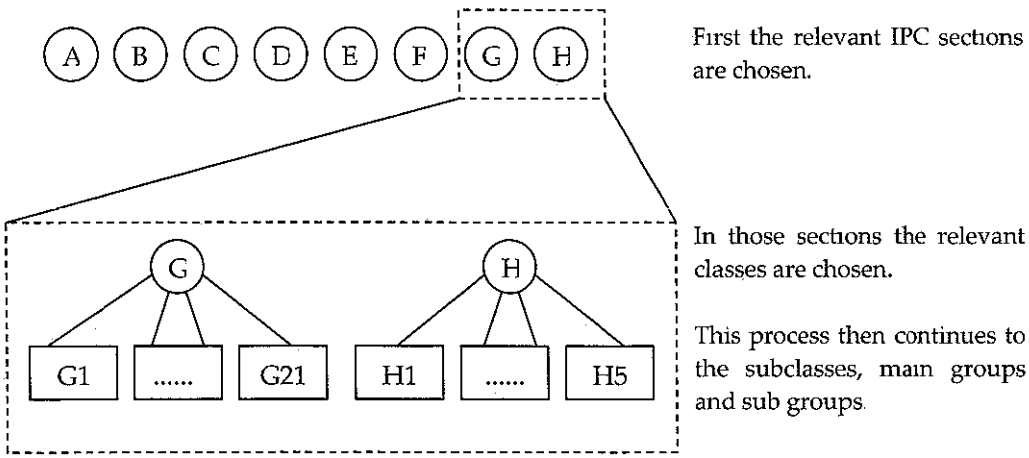


Figure 4.8. Illustration of hierarchical nature of IPC

The second approach of determining the classification of patents known to cover DRM technologies uses the patents found using Query 1. As the results of this query contain a large number of DRM patents, studying the classification of these patents can give insight into which classes are commonly assigned to DRM patents (see Figure 4.9, on the next page).

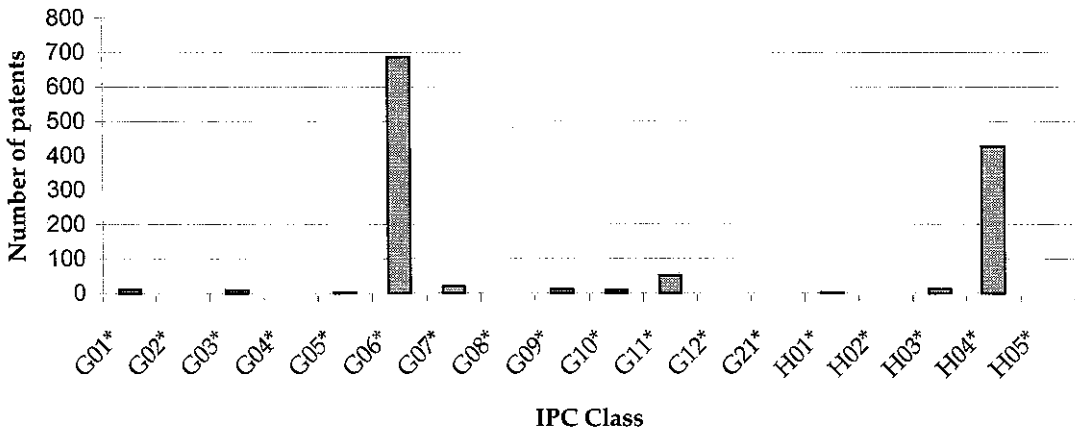


Figure 4.9. Results of Query 1 grouped per IPC class[43]

As can be seen in Figure 4.9, some classes are typically assigned to DRM patents, while others are not. The patents in the results of Query 1 show that DRM patents are often assigned class G06, which covers computing inventions, and class H04, which covers electric communication.

Using these different approaches a list is made of the IPC and ECLA classes that cover DRM patents (see Appendix B). The list is tested in several stages of development to verify that filtering the results of a query based on the IPC and ECLA classes in this list does not decrease completeness and does increase soundness. As the ECLA is a more detailed and consistently applied classification, filtering using the ECLA is a more prudent option than filtering using the IPC. However, not all patents have an ECLA code assigned to them. Patents that have no ECLA assigned to them will be filtered using the IPC.

4.4 Searching Using the Names of Inventors

The search using the names of inventors starts with creating a list of people that work for Philips that could be mentioned on patents that cover DRM technologies. A list consisting of three parts is made containing the names of the inventors of the patents that are assigned certain classes of the Philips internal patent classification. The first part is based on names of inventors listed on patents that have been classified internally as DRM, watermarking or fingerprinting[44]. The second and third parts cover the names found on patents classified as dealing with copy protection and such.

---

[43] For classes in sections G and H only. As one patent can be assigned more than one IPC code adding the number of patents in each class does not return the total number of patents in the results of Query 1.

[44] A list of patents classified as DRM in the Philips internal classification is not made, as this column would have only one name in it (EPSTEIN M).

A researcher in the field of DRM and a patent attorney that handles DRM patents on DRM technology then review this list[45]. Using their comments the list is fine-tuned. Names on the list that neither the researcher nor the patent attorney are familiar with are removed. The patents that bear one of the names of the inventor that are left and are assigned to Philips are retrieved. These patents are then manually reviewed to determine which could be DRM patents. This list of possible DRM patents is then compared to the patents assigned to Philips in the results of Query 3. Patents in the list based on inventor names that are not in the results of Query 3 are reviewed more carefully. Three DRM patents are found this way that were missed by Query 3. This makes the query accurate enough for reaching the goals of this research.

4.5 Results of the Search

Using Query 3 a list of DRM patents is made containing one patent per family[46]. The list does not contain equivalents therefore, which means that a single patent cannot appear on the list multiple times (e.g. the same patent listed once as a WO application and once as a EP patent). As a result, patents are also removed if they stem from the same application, but are essentially different. An example of when this can happen is when a single patent application has been split into two different applications, because the patent essentially covers two different inventions. In that case both patents stem from the same application and will therefore be seen as family, meaning one of them will be removed from the results. Such cases are exceptions though and developing a patent strategy for Philips' DRM patent portfolio does not depend on finding every single patent. An additional search is conducted in which equivalents are not automatically removed for just Philips' DRM patents (see Appendix D). The results of this search can be used by Philips to make more specific choices regarding a single or a few patents, whenever it is essential to work with a complete list of patents.

The results contain granted patents as well as patent applications. As applications can be turned down, it would technically be incorrect to treat these like granted patents. However, applications give a strong indication of what research a company is involved in. In the context of this research it is therefore wise to include applications in the process of comparing portfolios. In the discussion of the different companies and their patent portfolios (see §5.3) comments can be found that discuss the relevance of this choice.

[45] These are Mr. Frank Kamperman and Mr. Arnoud Engelfriet, respectively.

[46] These equivalents are automatically removed from the results by the search database.

Figure 4.10 (see below) shows the final and intermediate results of the process of the search for DRM patents. The results of Query 3 are split into two groups: one group of patents with an ECLA and one group of patents without an ECLA. The first group is filtered using the ECLA classification the second group is filtered using the IPC classification.

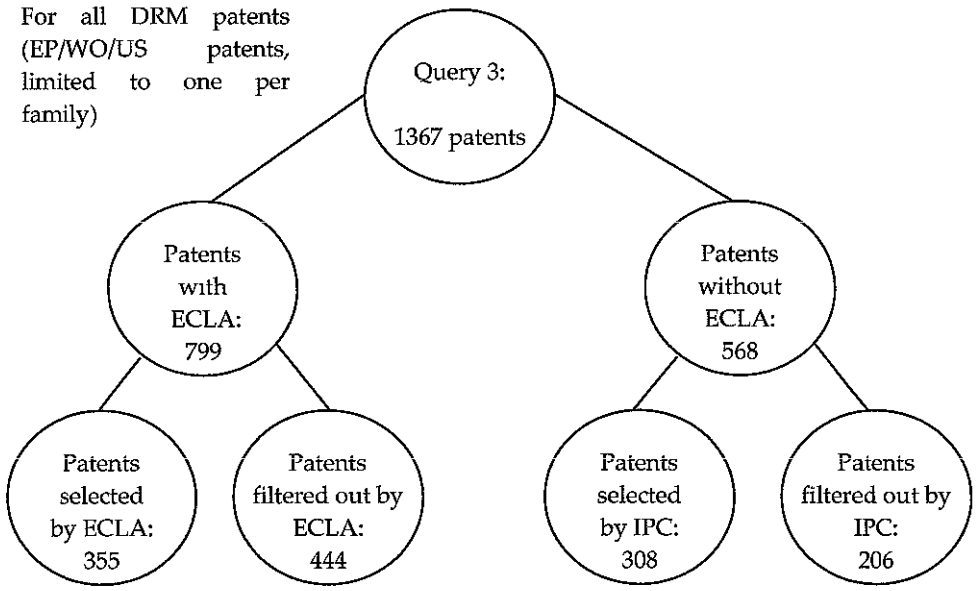


Figure 4.10. Results of Query 3 and filtering for all DRM patents

The total number of patents in the results of the search is 663 (355 selected by ECLA plus 308 selected by IPC). Some of these patents will not turn out to be DRM patents, because the filter is not fully accurate. These are known as false positives and will be removed if they're manually reviewed. This is the case for those patents that are assigned to the companies that are selected in the next chapter.

Patents that the filter removes but should not remove are known as false negatives. If the filter has a large false negative rate, then some important patents might be missed. A short review of the list of patents that are filtered out, shows that there are no large amounts of DRM patents in these results. Furthermore, the false positive and false negative rate for both the ECLA and the IPC filter are low (less than 10%) for the Philips patents in the results[47]. Assuming these rates are representative of the false positive and false negative rate for the complete results, these results are accurate enough for use in this research.

[47] These are the results of the additional search that is conducted for Philips DRM patents, where the "one per family option" is not selected.

5 Comparing Patent Holders and Their Portfolios

In this chapter the results of the search are used to select a number of companies so these companies and their portfolios can be compared to Philips and its portfolio. The comparison of these companies will include factors such as company size and alliances between DRM patent holders. The DRM patent classification is used for the comparison of the patent portfolios.

At the end of the chapter a discussion is presented of what parts of the comparison are relevant to Philips.

Contents of this chapter:

5.1 Selecting the Patent Holders to Compare

Due to the large number of DRM patents found, it is impossible to review every patent to determine a patent strategy. This is however not necessary as the strategy is focused on a company's whole portfolio and not on single patents[48]. Therefore only a limited number of patent holders will be included in the comparison of patent portfolios. Using the additional search results and other data available in the appendixes, Philips can use its own (classified) intelligence to tailor the patent strategy suggested in this research (see Chapter 6) to specific situations involving a single or a few patents.

The search for DRM patents delivers a list of 663 patents after filtering based on ECLA and IPC. Of these patents, 175 have no assignee and are as such removed from the list[49]. The plot in figure 5.1 (next page) shows the patentees holding three or more patents and there clearly are three different groups distinguishable. The second and third group are selected for review and these include all assignees that hold more than ten patents. Most of Philips' major competitors (e.g. Sony and Matsushita) and some other important DRM patent holders (e.g. InterTrust and ContentGuard) are included in this second and third group. However, an additional number of DRM patent holders are selected that hold few DRM patents, but might still be of importance. These include patent holders that seem relevant because of their association with other companies that are selected or with emerging DRM standards.

The companies that are selected based on the number of DRM patents they own (over 10 patents) are introduced in the next section (see figure 5.2). It is important to realize that some of these companies hold more patents than the ones found, as the search was limited to one patent per family[50].

---

[48] The major, yet unlikely, threat that stems from not reviewing each and every single patent holder is that such a patent holder holds a relatively important patent and licenses it to only a certain number of companies (e.g. Philips competitors). Such risks are however inevitable, cannot be foreseen and would therefore likely not influence the choice for a certain patent strategy. Besides, these minor details do not outweigh the unsurpassable threat of the lack of transparency that comes from the long delay in firms applying for a patent and the first publication of the application.

[49] It is not obligatory, when applying for a patent, to indicate whom the assignee will be. However, in some of these cases the assignee had not yet been entered into the database in Pluspat for an unknown reason. As it is too time consuming to manually add the missing data to the list of patents using another database, these patents are omitted. A random review of 15 of these patents indicated that most of these patents are held by individual inventors.

[50] InterTrust has 26 issued United States patents according to itself, however: "many of the company's patents are embodied in a very large omnibus patent application filed in February 1995" [InterTrust.com, b]. This explains why fewer patents show up in a search limited to one patent per family. It is not necessary to review the patents in InterTrust's portfolio that are not part of the search results, as a short inspection shows that they are similar to the once that are part of the search results.

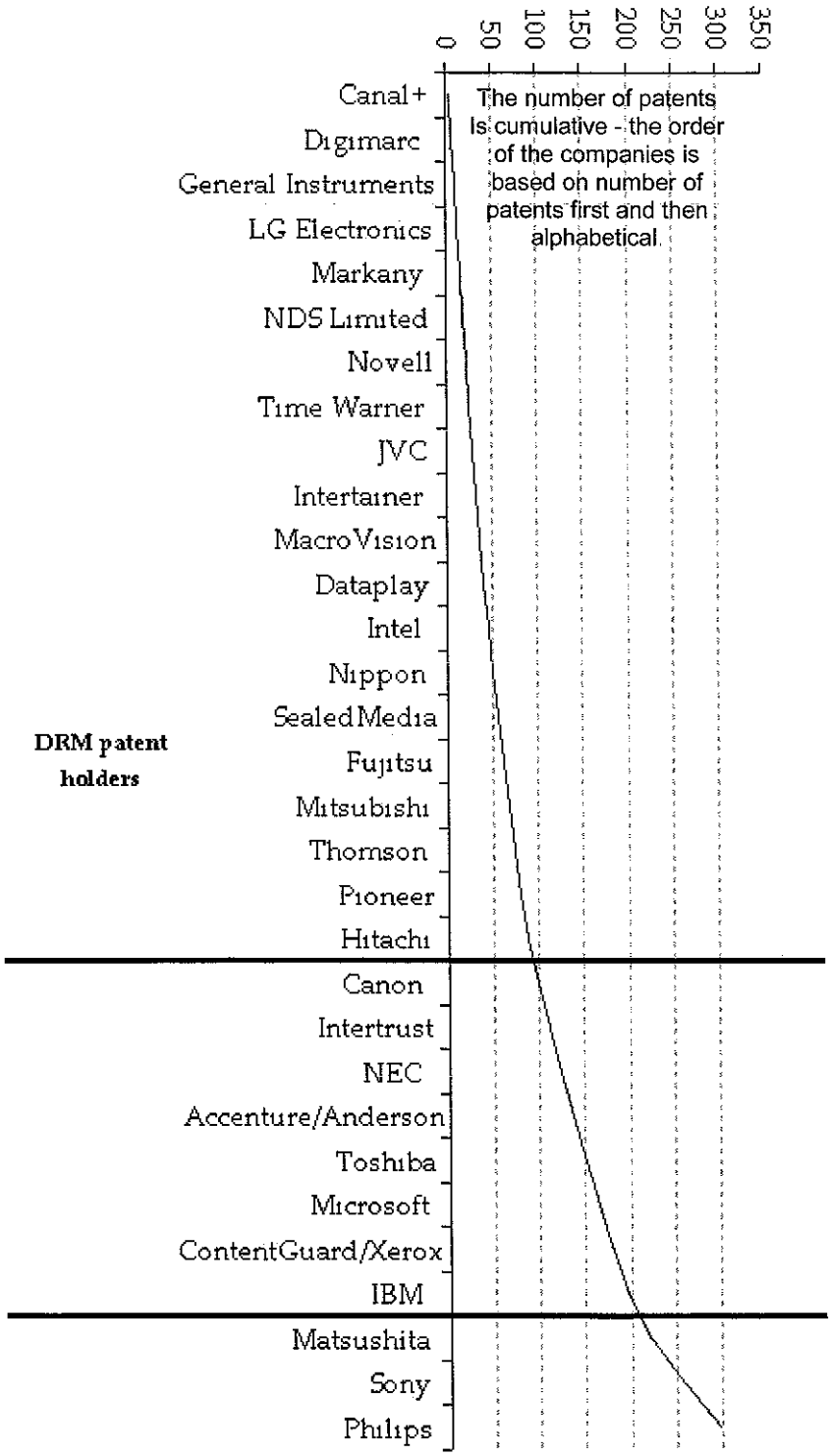


Figure 5 1. Selecting DRM Patent Holders Based on Portfolio Size

Company	Description of the company
Accenture 14 patents[51]	Accenture (prior to 2001; Anderson Consulting) is a consultancy firm that also does research and development (R&D) in emerging technologies. The focus of this R&D is on business problems and business solutions.
Canon 11 patents	Canon mostly produces video, photography and image processing equipment for personal, business and industrial use [Canon.com].
ContentGuard 16 patents	ContentGuard was launched in April 2000 and is owned by Xerox and Microsoft, with the latter holding a minority position. The company's patent portfolio consists mainly of patents on technologies related to rights grammars that were developed at Xerox Palo Alto Research Center (PARC) [ContentGuard.com].
IBM 16 patents	IBM produces all kinds of computer equipment ranging from personal computers to large server networks and offers a range of mainly business software products as well as consulting and infrastructure services [IBM.com].
InterTrust 12 patents	InterTrust is a company that holds a substantial number of very broad patents to DRM and was one of the first companies to apply for patents on DRM technologies. The company was founded in 1990 and has since then produced some DRM software products.
Toshiba 14 patents	Toshiba produces a wide array of products, including (consumer) electronics, information and communication systems and computers, but also medical equipment and heavy electrical apparatus.
Matsushita 26 patents	Matsushita is most well known for its Panasonic brand, but also has some other brands in its home-country Japan that are of no interest here. Panasonic makes consumer electronics much like Philips does.
Microsoft 14 patents	Microsoft is the world's largest software manufacturer and produces the operating system that is used on more personal computers than any other. Within this company the focus is on using DRM technologies in operating systems, providing a trusted environment for content.
NEC	This is a special case, as the search returned 12 patents, yet a review of these patents shows that five of these do not cover DRM technologies. As such NEC will not be selected based on the number of DRM patents it has.
Philips 42 patents	Philips is Europe's largest and the world's third largest producer of audio / video consumer electronics. Conditional access, digital television and broadcasting, digital set-top-boxes and several digital audio and video formats are some of the fields in which Philips products can be found.
Sony 35 patents	Sony is one of Philips major competitors, but also a partner in the development of certain standards (e.g. CD and DVD). It is active in many of the fields that Philips is active in, but unlike Philips still owns record and movie labels and therefore likely has more interest in implementing DRM in consume electronics.

Figure 5.2: Selected companies holding ten or more DRM patents

[51] The number of patents in this column are the number of patent that were found through the search. Some of these patents will later turn out not to be DRM patents according to the definition used in this paper

Six additional companies, other than these companies holding ten or more DRM patents, are selected for further review (see figure 5.3 below). This additional selection of companies is very diverse and adds to the list:

- Two companies that provide merely DRM or DRM enabling technologies (SealedMedia and DigiMarc respectively);
- One company that traditionally produces copy protection technologies (MacroVision);
- Two smaller consumer electronics companies (Thomson and Hitachi); and
- One additional company from the computer industry that seems to have in interest in DRM (Intel).

An introduction to these companies is found below (figure 5.3).

Company	Description of the company
DigiMarc 3 patents	DigiMarc produces digital watermarking technologies, which can be used in DRM systems.
MacroVision 4 patents	MacroVision is very strong in copy protection technologies and likely has an interest in DRM technologies therefore[52].
Intel 5 patents	Intel is strong in the computer hardware industry and is part of some DRM alliances[53], indicating interest in DRM.
SealedMedia 5 patents	SealedMedia provides a DRM product for managing documents in a computer network environment[54].
Thomson 6 patents	Thomson is a smaller producer of consumer electronics, but it holds a strong position in video broadcasting and is part of some DRM alliances[53].
Hitachi 8 patents	Hitachi is a smaller producer of consumer electronics, which does not hold a particularly strong position in any field related to DRM yet is also part of some DRM alliances[53].

Figure 5.3: Additional selection of companies

This brings the complete list of companies that are selected for a comparison to a total number of 15 (see figure 5.4):

Holding more than 10 DRM patents		Selected for other reasons	
• Accenture	• Microsoft	• Digimarc	• SealedMedia
• Canon	• Philips	• MacroVision	• Thomson
• IBM	• Sony	• Intel	• Hitachi
• InterTrust	• Toshiba		
• Matsushita			

Figure 5.4: List of selected companies

[52] Similar companies, such as Canal+ and Nagravision, are not selected.

[53] See §5.2 for a discussion of these alliances.

[54] According to itself, SealedMedia is "a software developer that provides a Document Security solution [...] allowing originators to change rights to access and use information" [SealedMedia.com]

5.2 Comparing DRM patent holders

5.2.1 Comparing General Features

There are many features of the selected companies that can be compared. Most such features are however only relevant when developing a business strategy or a market strategy. Therefore, the factors that influence patent strategies that are discussed in §2.3 and §2.4 are used for this comparison (e.g company and portfolio size and the ability to produce multi invention products).

It would be best to look at income and licensing revenues from DRM operations to compare the size of these selected companies. However, most companies do not produce any DRM products[55] and little to no data is available on licensing revenues. Therefore, a comparison will be made based on total revenues instead (figure 5.5).

Comparing companies based on the size of their total revenues[56]		
Approx 10 - 100 **million** dollar range	Approx. 10 - 80 **billion** dollar range	
• DigiMarc • InterTrust • Macrovision • SealedMedia	• Accenture • Canon • Hitachi • IBM • Intel • Matsushita	• Microsoft • Philips • Sony • Thomson • Toshiba • Xerox

Figure 5.5: Revenues of selected companies

It is clear that the companies that do not produce any products themselves, but merely license technologies, have far lower revenues than those companies that do deliver products and/or services. This makes these non-producing companies easier targets for a merger or acquisition. It also makes it more difficult for these companies to start lengthy litigation unless they receive great financial support, for instance from another company.

---

[55] Besides SealedMedia, Microsoft and IBM also already offer DRM solutions, yet no information is available on the scale in which these are implemented or licensed. Microsoft offers Windows Rights Management Services, which focuses on document management at this time. In the near future Microsoft plans to provide a "Unified DRM" technology, which will incorporate audio, video and data into a single DRM solution [DRM Watch, a]. IBM is offering its xCP content protection technologies and its Electronic Media Management System (EMMS). The first is a cluster protocol that can be implemented in home networks for DRM purposes. The latter is a complete DRM solution for PC platforms [DRM Watch, b].

[56] All data taken from the 2002 annual reports: Accenture 13b$; Canon 24.5 b$; IBM 81.1 b$; Matsushita 51 b$; Microsoft 28 b$; Philips 31.8 b€; Sony 57 b$, Toshiba 40.6 b$; DigiMarc 86m$; SealedMedia N/A - but very unlikely to be in the billion dollar range, Thomson 7.8b$; Intel 26.7 b$; Hitachi 68 b$, Macrovision 102 m$; ContentGuard has no annual report – we used Xerox 15.8 b$, InterTrust has no annual report on web site - we used the 2002 10-k available using EDGAR at sec.gov 8.4 m$

Companies do not invest the same amount, whether fixed or relative to revenues, in patenting and licensing operations or in detecting infringement and subsequent patent litigation. It would be best to compare the number of patents owned, the licensing revenues made and the number of patent lawsuits that are won or settled. Again, such information is difficult or impossible to obtain and therefore only the total number of patents owned by each company will be compared.

To find the total number of patents the United States Patent and Trademark Office (USPTO) database is used, which is available through the USPTO website[57]. The results will not be completely accurate, as some companies own patents that have an assignee that is different from their own name and some names might be used by multiple unrelated companies. The results are however accurate enough to show the magnitude to each company's portfolio (see figure 5.6).

Comparing companies based on the size of their total patent portfolio[58]	
< 100	SealedMedia, InterTrust, Accenture, DigiMarc and Macrovision
< 5.000	Microsoft
< 10.000	Intel and Thomson
< 20.000	Matsushita, Philips, Sony, Toshiba and Xerox (ContentGuard)
< 30.000	Canon and Hitachi
< 40.000	IBM

Figure 5 6: Patent portfolios of selected companies

The list of DRM patent holders contains both companies from the consumer electronics industry and companies from the computer hardware and software industries. Some of these companies provide technologies that are also used in products that are to some extent already a product of digital convergence. The most important example here of such convergence are digital television set-top-boxes, which are consumer electronics using partially generic hardware and using standardized software components. The importance of each company to each of these fields is indicated in figure 5.7.

---

[57] This limits the search to US patents to give more weight to different patents than to similar patents in different countries. As important inventions are typically patented in the US by all companies wherever their headquarters may be, it should not skew the results too much to US based companies.

[58] All searches used www.uspto.gov/patft: Accenture / Anderson Consulting: 65 + 3; Canon 27.043; Hitachi 28.101; IBM 527 + 34.377, Intel 7.312; Matsushita 19.521; Microsoft 2.825; Philips 18.529; Sony 18.207, Thomson 8.186; Toshiba 19.845, ContentGuard / Xerox 2 + 15.004; DigiMarc 106, ,InterTrust 22; Macrovision 68; SealedMedia 0 (Search in Espacenet delivers 5 WO patents).

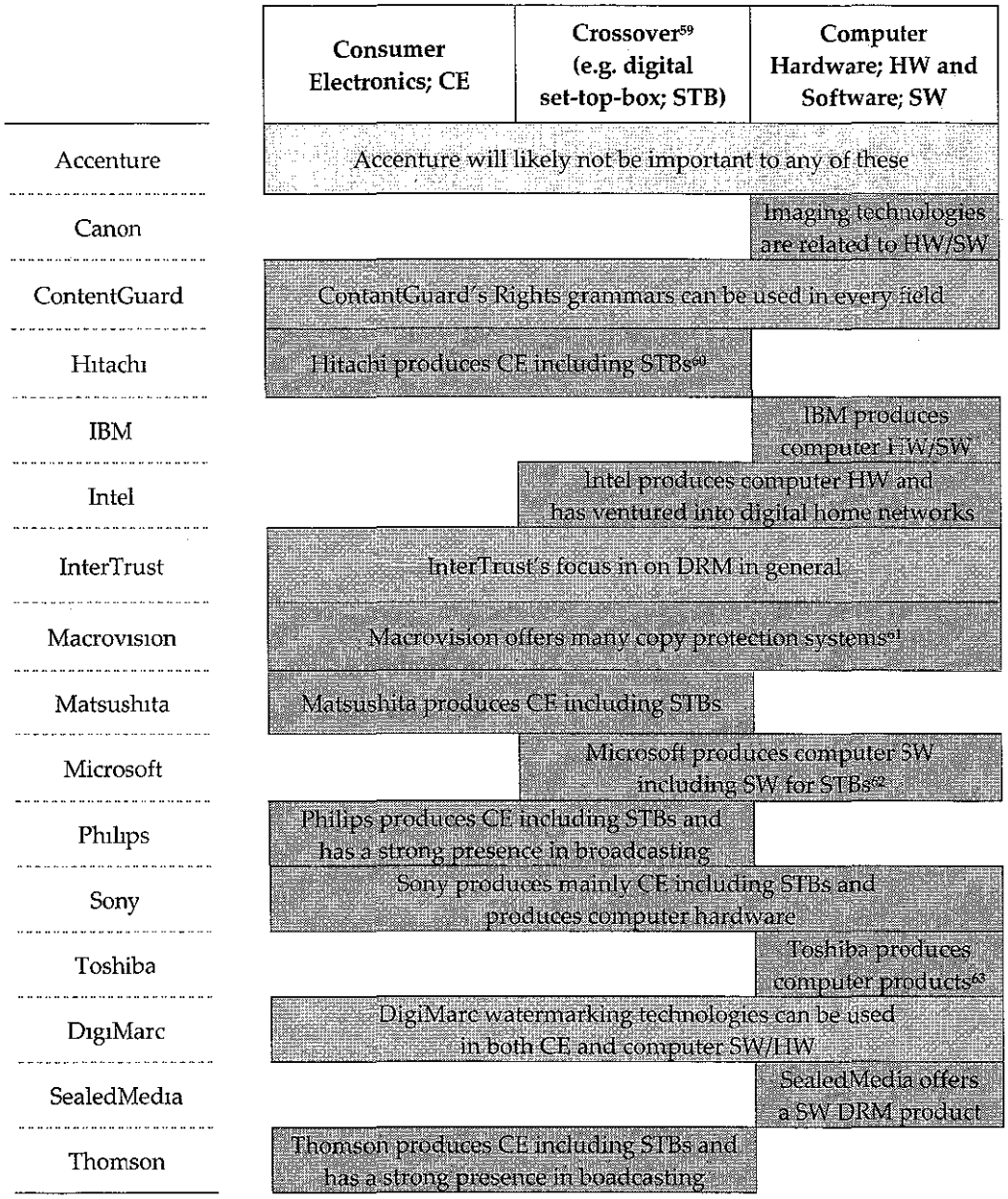


Figure 5 7: "Industry" the selected companies belong to

[59] Crossover products are a convergence between consumer electronics and computers. A digital STB is an example of such a product as it connects to CE and typically has general HW and a layered SW model like computers have.

[60] Hitachi produces some computer products (e.g. servers), but very little compared to its line of consumer electronics.

[61] Although Macrovision's traditional products are analog copy protection systems not considered DRM in this paper, the company is venturing into the digital world.

[62] Microsoft also sells computer HW that is produced by others and then labeled as Microsoft products, yet it its core activity is SW with a focus on operating systems.

[63] Toshiba produces some consumer electronics, but very little compared to its line of computer products.

As the previous figure shows, all consumer electronics companies that have been selected offer digital STBs. This should not be a surprise, as these companies are likely developing and patenting DRM technologies because they are producing such crossover products.

Most of the selected companies will be able to produce complete DRM systems. For others this entails outsourcing the manufacturing or producing only the software that is needed to turn a generic device (e.g. a computer) into a DRM capable system. Some companies however, are likely to produce only parts of DRM systems or not produce anything at all and merely license their DRM technologies. Of course a company that can produce a complete DRM system can also produce parts or license DRM technologies. Similarly a company that is able to produce parts of a DRM system can choose to license DRM technologies.

This is an overview of all the selected companies and an estimate of their abilities:

- The companies likely to produce a DRM system are: Hitachi, Matsushita, Microsoft, Philips, Sony and Thomson. All of these produce STBs with the exception of Microsoft, which produces software for STBs and can outsource the manufacturing.
- The companies that are unlikely to produce complete DRM systems, but manufacture parts of a DRM system are: Canon, IBM, Intel, SealedMedia[64] and Toshiba. All of these can manufacture semi-conductors or software components for DRM systems.
- Finally there are a few companies that will likely only license DRM patents: Accenture, ContentGuard, DigiMarc and InterTrust[65].

[64] SealedMedia will likely only produce DRM systems for document management like it does now.

[65] InterTrust produces DRM software solutions, yet it seems to have more interest in licensing its technology.

5.2.2 *Standardization Alliances Between DRM Patent Holders*

There are several alliances between the DRM patent holders that were formed to standardize (elements of) DRM systems [Lyon, 2002]. Some of these alliances include the creation of a patent pool, indicating that companies are likely willing to license to create scale advantages for the standard. The most important alliances are discussed and a matrix is presented towards the end of the paragraph that shows the members for each alliance (figure 5.8).

Secure Digital Music Initiative (SDMI)

The SDMI initiative has more than 150 participants including consumer electronics manufacturers, computer software and hardware manufacturers and content creators. The SDMI initiative failed to bind all these different participants to a single technology In fact the proposed copy protection technology using watermarking could easily be circumvented and as of May 18th, 2001 SDMI is in hiatus.

Digital Transmission Content Protection (DTCP)

DTCP is a specification of a system that protects content transfer over FireWire (implementations for USB and over IP networks are in the process of being added). The system includes copy control information and authentication and revocation of (compliant) devices [DTCP.com]. DTCP technology is part of a complete DRM solution and is implemented in consumer devices that receive content (e.g. a set-top-box) and transfer this content to other devices (e.g. displays). The Digital Transmission Licensing Authority has been established by the five companies that developed DTCP to license the technology.

Internet Streaming Media Alliance (ISMA)

ISMA is a "non-profit corporation formed to accelerate the market adoption of open standards for streaming rich media over Internet Protocols" [ISMA.tv]. This organization is currently focused on creating a MPEG-4 based standard for content distribution over IP networks. DRM is an important aspect in the specifications ISMA is developing.

Content Protection for Recordable Media and Pre-Recorded Media (CPPM /CPRM)

"The CPRM/CPPM specification defines a renewable cryptographic method for protecting entertainment content when recorded on physical media." [4Centity.com] The companies involved in this specification (together knows as the 4C Entity) have also developed a DRM architecture and an audio watermark and are currently developing a video watermark. The audio watermark is in fact the one that was selected by the SDMI for its Phase 1 portable device specification.

Copy Protection Technical Working Group (CPTWG)
The CPTWG is a cross-industry working group holds monthly meetings with consumer electronics manufacturers, hardware and software manufacturers, cable and satellite television companies, content creators and lobby groups of several organizations. The CPTWG does not produce any standards itself and it seems to include in its meetings all the companies holding DRM patents and other companies with an interest in DRM.

Digital Video Broadcasting (DVB)
Within the DVB group a Copy Protection (CP) group and Copy Protection Technical (CPT) group have been formed [DVB.org]. Together these try to realize a system for content protection and copy management (CPCM). The DVB standards are compulsory for digital video broadcasting in Europe, yet the group is an industry initiative. As the DVB standards are at the front of the convergence between consumer electronics and computers, this group includes companies from the consumer electronics as well as from the computer hardware and software industries.

SmartRight
This system developed by Thomson is an extension to a conditional access system. It encrypts content, specifically video, when entering the home (e.g. through a set-top-box) and within a "home network" content can be stored in encrypted form using "normal" devices. Content can then only be played within this home network with devices coupled to a decryption module. This system can be seen as an intermediate step between conditional access systems and DRM.

High-bandwidth Digital Content Protection (HDCP)
The HDCP specification covers a technology that protects content transfer over a Digital Visual Interface (DVI), which is most frequently used to connect a computer to a flat-panel monitor [Digital-CP com]. The Digital Content Protection organization has been established by Intel, which created HDCP, to license the technology.

TV Anytime Forum
"The global TV-Anytime Forum is an association of organizations which seeks to develop specifications to enable audio-visual and other services based on [...] local storage" [TV-Anytime.org]. The name TV Anytime refers to this local storage element, as storing received content locally enables consumers to use this content when they want to (e.g. watching a movie broadcast on TV at a later time). The forum, which includes a working group on DRM, consists of approximately 60 members including broadcasters, consumer electronics companies and computer software manufacturers.

Others
There are several other groups that are focused on creating languages or meta-data standards that can be used in DRM. Patents rarely cover such standards and languages.

	Digital music	Content over IP	Securing content on CD/DVD	Content transfer between devices		Digital television	
Member of:	SDMI[66]	ISMA	4C Entity CPPM / CPRM	HDCP	DTCP	DVB CP / CPT	TV Anytime
Accenture							
Canon							
ContentGuard							Y
Hitachi	Y	Y			Y		
IBM	Y	Y	Y				
Intel	Y		Y	Y	Y	Y	
InterTrust	Y						
Macrovision	Y					Y	Y
Matsushita	Y	Y	Y		Y	Y	Y
Microsoft	Y					Y	Y
Philips	Y	Y				Y	Y
Sony	Y	Y			Y	Y	Y
Toshiba	Y		Y		Y	Y	
DigiMarc	Y					Y	
SealedMedia							
Thomson	Y	Y				Y	Y
	12	6 - Mostly consumer electronics companies	4 - Mostly computer companies	1 - Only Intel	5 - Mostly computer industry	9	7

Figure 5.8: Matrix of alliances between selected companies

This matrix (figure 5.8) shows that:

- Accenture, Canon and SealedMedia are not in any of these groups. Likely their R&D is not focused on any DRM solutions that are of major importance to any of these groups or their members.
- Every selected company that is a member of any other group is also a member of the SDMI group. Taking this into account as well as the fact that this group has gone into hiatus, it seems the SDMI it is of little importance.
- All consumer electronics companies, except Hitachi, are in the two digital television groups. To these companies digital television is probably one of the most important growth markets for the near future.
- The only group, in this list, that focuses on online content distribution has more consumer electronics companies as members than computer companies. Perhaps the computer software companies are not interested in the emergence of standards and would rather push proprietary technologies.
- None of the groups are made up completely out of consumer electronics companies. Several companies are however made up out of mostly computer hardware and software companies.

[66] Source: SDMI.org

A look at the number of these groups that each company is in shows that the companies that are likely to produce their own DRM systems are in more groups than those that are likely to license or produce only parts of DRM systems (see figure 5.9).

Number of groups a company is in and the likeliness that it will produce DRM systems	
	Likely to license (except Canon and SealedMedia)
0	Accenture, Canon and SealedMedia
1	ContentGuard and InterTrust
2	DigiMarc
	Likely to produce parts of DRM systems (except Microsoft)
3	Hitachi, IBM, Macrovision and Microsoft
	Likely to produce complete DRM systems (except Intel)
4	Philips, Toshiba and Thomson
5	Intel and Sony
6	Matsushita

Figure 5.9: Comparing likelihness to produce and alliances

5.2.3 *Other Alliances and Relationships Between DRM Patent Holders*

There are a few other alliances between companies that seem relevant in determining a patent strategy. The alliance between Philips and Sony that has lead to the success of the CD and DVD seems relevant, as these media are dominant for digital audio and video. These companies produce a large part of the world's consumer electronics and will likely implement DRM features in these products in the future.

Another alliance that seems relevant is the share Microsoft has in ContentGuard. This seems to indicate that Microsoft wants to use a complex rights grammar, likely based on eXenteded Markup Language (XML). If Microsoft can push such a language as a standard it can use its partial control over ContentGuard to get even more leverage.

There's more to be said about Microsoft as the company is currently involved in litigation with InterTrust, which claims that Microsoft's products, including several versions of Windows and Windows Media Player, infringe its patents. The outcomes of this case is uncertain at this time, yet it seems likely that if the case is not settled it will last several years. At the same time, the effects of the Microsoft anti-trust cases in the United States and the European Union on the company are not yet known.

5.3 Comparing patent portfolios

To compare the patent portfolios of the 16 companies that have been selected, each patent is reviewed, summarized and assigned a class in the DRM classification (see §3.5 for this classification and appendix C for the summaries and such). The portfolios are discussed below in figure 5.10 (continues on the next page). In this figure the darkness of the color indicates the importance of the portfolio. There are three gradations, which indicate above average importance (dark gray), about average importance (light gray) and below average importance (white).

Company	Description of the DRM portfolio
Accenture	Patents seem irrelevant to consumer electronics, as they are focused on the business side of financial aspects of DRM systems.
Canon	Patents cover watermarking technologies in digital video and should be seen as patents on DRM enabling technologies.
ContentGuard/Xerox	Patents cover some core aspects of DRM, such as the association of usage rights to content, the use of a grammar to define rights and some fee accounting and reporting mechanisms. The portfolio also contains some enabling technologies for content protection.
Digimarc	Patents focus on different aspects of watermarks including embedding the watermark and identifying content based on a watermark.
Hitachi	Patents focus on access control to documents. The portfolio also includes patents to various aspects of DRM systems such as payment methods, compliancy management and trusted systems. It seems the portfolio covers more DRM aspects for computer software than for consumer electronics
IBM	Patents are very diverse ranging from single technologies to track usage or collect royalties to complete systems (e.g. IBM's Cryptolope system). It seems unlikely that IBM's patents are essential to most DRM systems, however the diversity of the portfolio increases the chance that IBM holds some technologies that might be valuable.
Intel	Patents focus on securely transferring content between devices, which is not surprising as Intel is active in the HDCP and DTCP alliances.
InterTrust	Patents cover some critical aspects of DRM in general including the use of trusted systems and content and rights distribution. The portfolio also contains some more specific patents on using watermarks, for example, for content authentication and on secure storage and business methods. The general nature of InterTrust's patents make it very likely that some of these patents are essential to most DRM systems.
Macrovision	Patents focus on copy control systems using different technologies. It seems the portfolio is a result of the continuation of Macrovision's research in copy protection using new technologies.

Figure 5.10: Comparing portfolios

Company	Description of the DRM portfolio
Matsushita	Patents cover both technologies focused on secure content distribution and copy control using optical disks as well as some rights management aspects of DRM systems (e.g. using licenses and separate transmission of content and rights). The portfolio is diverse covering both copy control and more advanced DRM technologies.
Microsoft	Patents cover some DRM architectures and more specifically content handling parts of trusted systems. The portfolio contains a variety of patents covering encryption methods and key distribution.
Philips	Patents are very diverse covering mostly aspects of distribution of content, revocation, Philips' complete data set technology[67] and copy control systems. Some other patents cover circumvention technologies, technologies to prevent circumvention and methods for securely transferring content between devices.
SealedMedia	Patents are diverse and likely cover some technologies used in the computer based DRM system SealedMedia produces. Two patents in the portfolio cover the creation of a trusted system.
Sony	Patents are focused on copy control systems including some patents on embedding copy control information using watermarks. The portfolio also contains patents on key management and some DRM architectures which enable royalty payment.
Thomson	Patents focus on securely transferring content between devices.
Toshiba	Patents focus on secure content distribution and copy control using optical disks.

Figure 5.10 (continued from previous page): Comparing portfolios

This comparison shows that most companies hold a varied portfolio. There are however several concentrations noticeable, besides the obvious concentrations in the portfolios of InterTrust and ContentGuard. These concentrations are:

- Patents on content protection technologies are most frequently found in the portfolios of consumer electronics companies, yet Microsoft also has a number of patents in these technologies.
- Only Philips seems to have several patents on content authentication technologies, yet these are almost all on one technology (complete data set technology).

[67] The "complete data-set" technology is a content authentication technology. In order for a compliant device to play a CD, DVD or another media, the complete content must be present on the media. For example, all the songs on a CD must be present, preventing the use of, for example, a copy of a single song. This makes it more difficult to copy songs that were downloaded of the Internet onto a CD, as one would need to get all the songs for the CD to play.

- Philips and Thomson hold a relatively large number of patents on device (compliance) management patents.
- Many consumer electronics companies hold patents on copy control systems, which are primitive DRM systems. Specifically Sony's portfolio has a high concentration of patents on this technology.

All the information about the portfolios of the selected companies and the alliances between these companies can be used to determine Philips's position. This is done in the next section (§5.4)

5.4 Relating the Comparison to Philips

Philips' position amongst other patent holders seems to equal that of most other consumer electronics companies. At the same time, there are some unique characteristics to Philips position. The position of the consumer electronics companies, including Philips, can be characterized as follows:

- Patent portfolios are of a varied nature and of average importance. There is no consumer electronics company that can dominate over another company based merely on the patents it holds.
- DRM technologies will be used in a multitude of products and access is therefore needed to InterTrust's patents and perhaps ContentGuard's patents as well.
- Standards are essential for DRM to become a success, because of interoperability reasons. All of these consumer electronics companies are therefore active in several alliances
- All consumer electronics companies will face new competition due to the digital convergence Not all of these new competitors, specifically the computer software manufacturers, are known for their cooperation in standardization.

This part of the comparison indicates that the consumer electronics companies have several common goals. Then there are the unique aspects of Philips position:

- Philips has several patents in content authentication technologies, although most consumer electronics companies only hold content protection patents in the content management patent class.
- Philips and Thomson are the only consumer electronics companies holding patents on device compliance management.
- Philips has close contacts with Sony, which holds many copy control patents. Such patents in combination with the content protection patents that most consumer electronics companies hold cover most aspects of simple DRM systems.

This second part of the comparison again shows that cooperation between companies is essential. It also shows that Philips and Sony together hold a strong position. It is possible that these two would lead an industry effort in standardizing (elements of) DRM. Different options are presented in the next chapter, in which the patent strategy for Philips is determined.

6 Conclusion: Determining the Strategy

In this chapter the patent strategy for Philips DRM portfolio is determined based on the information gathered throughout this research paper. The strategy choice model is used in the first section to derive a general strategy for the portfolio. In the next section all the market and technology specific and other relevant factors for DRM are used to fine tune the strategy. All of the sections in this chapter use the results of the comparison of the selected companies and their portfolios (see Chapter 5).

At the end of the chapter a summary of the strategy is presented together with some remarks on the use of the strategy.

Contents of this chapter:

6.1 Using the Strategy Choice Model

To determine Philips' position in the strategy choice model, the willingness to license and the importance of Philips' portfolio have to be estimated. The willingness to license is large, because Philips typically uses RAND licensing for all its patents[68] and like most other companies Philips will not be able to produce a DRM system without infringing some other company's patents. An isolation strategy is therefore not possible for most companies. The companies that hold the most important portfolios, InterTrust and to a lesser extent ContentGuard, both depend on licensing revenues and are therefore likely to license.

Finally, the standardization of DRM technologies is essential for interoperability, which is essential to the success of such technologies. The widespread use of a standard requires companies' to license their patents to the technologies used in this standard.

Philips' portfolio is above average importance, although it does not quite compare to InterTrust's portfolio or ContentGuard's portfolio, it does have some strong features in content protection and content authentication technologies. Furthermore, Philips' portfolio is rather large compared to most other portfolios[69]. The importance of Philips' portfolio in combination with the high willingness to license, lead the strategy choice model to advise a licensing strategy with some added defensive elements.

However, an isolation strategy could theoretically be used for Philips' complete data set technology, which stands out in the portfolio as it is relatively strongly protected. Yet, there are many other content authentication technologies available and the success of any such technology depends on the widespread use of it through standardization. This makes it unlikely that an isolation strategy for Philips' complete data set technology would be successful and a licensing strategy would therefore be advised for this cluster of patents as well.

The strategy choice model advises a general strategy, but does not provide the details that are needed in determining a strategy that covers patenting, licensing and enforcement. Furthermore there are many different strategic elements that can be added to the licensing strategy. These details require that the factors that influence patent strategy choice (§2.3 and §2.4) and the comparison of DRM patent holders and their portfolios (§5.3 and §5 4) are taken into account. The next section (§6.2) does exactly that.

---

[68] With the exception to patents on some products such as men's shavers.

[69] This could to some extent be the effect of the formulation of the search for DRM patents being more heavily influenced by Philips' view on DRM. However, the results also show that Sony's portfolio size is comparable to that of Philips portfolio (even more so if Philips' patents on its complete data set technology are counted as one)

6.2 Fine-tuning the Strategy

To fine-tune the strategy several factors that influence strategy choice are examined. The first two factors are the market and technology specific factors. The most important market specific factor is the convergence of consumer electronics and computers. Devices that support DRM will be at the front of this digital convergence. The companies that influence the use of DRM technologies will therefore come from computer hardware and software industries as well as from the consumer electronics industry. As such, Philips will have to keep track of more companies than for the typical consumer electronics product or technology. Add to this the technology specific factor, which is that DRM is a new technology that will be used in multi invention products, and it becomes clear that there is great uncertainty towards the future of DRM. This uncertainty calls for strong defensive elements in the patent strategy. At the same time this uncertainty pushes Philips and other DRM patent holders as well as other actors that are related to DRM (e.g. content producers) towards cooperating in order to overcome this uncertainty.

Other factors that influence strategy are company and portfolio size. These do not differentiate Philips from the other DRM patent holders. The cooperation between DRM patent holders that was mentioned in the previous section, can lead to the creation of standards and in fact here already are several such standards being created by alliances between DRM patent holders and other actors. Although these standards seem necessary for the technology to be successful, they also present a danger. A company that controls the standard setting process has great influence over other companies wanting to license DRM patents or use DRM technologies. It is unlikely that Philips can create a DRM standard that becomes dominant on its own. Likely, a standard will emerge that is under control of several companies. Although such multi-company standards are common for computer hardware (e.g. the Peripheral Connection Interface and the Universal Serial Bus), they are far less common for computer software. The most important company in computer software is Microsoft and specifically this company has used the control over standards in its favor[70].

The companies that could be most influential on the standard setting process based on their DRM portfolios are InterTrust and to a lesser extent ContentGuard. Yet, these companies do not benefit from one standard prevailing over another standard, when both such standards use their patented technologies. As InterTrust is a rather small, it is possible that a larger company takes control over this company (e.g. through an acquisition). Take Microsoft as an example, which already owns a part of ContentGuard. If this company would also get control over InterTrust, this would enable Microsoft to create and then push a standard to its liking.

[70] Microsoft has adapted existing standards in implementing them in its favor (e.g. JAVA and HTML).

Based on the factors that are discussed above, the elements that make up the combination of a licensing strategy and a defensive strategy can be described in more detail. The strategy is split up into patenting, licensing and enforcement elements, just like the general strategies in Chapter 2.

In a licensing strategy, patenting is typically not the most important element. However, when defensive elements are added it become the most important part of the strategy. It is unlikely that the creation of new patents will provide Philips with a position that is strong enough to leverage access to all (essential) patents. Still, an important element of patenting in this strategy is that inventions that are of importance to Philips' competitors are patented even if these technologies are not relevant to Philips' own products. The two companies that hold portfolio's to which access is essential (InterTrust and to a lesser extent ContentGuard), will not want a cross-licensing agreement. This requires that Philips use other methods to prevent either of these companies from blocking access to their patents. As Philips shares this goal with the other consumer electronics companies and with others as well, it is likely that some of these companies will unite to reach this common goal.

In a licensing strategy, the actual licensing is most important as the strategy is focused on exploiting the economic value of an innovation by creating revenues through licensing. In this strategy this value will most likely come from cross-licenses, as defensive elements will focus on creating freedom-to-operate, which typically results in cross-licensing. In licensing therefore, the optimization of licensing revenues through profit maximization is not relevant at this time. If Philips is able to get access to all patents that are essential to (a dominant standard for) DRM, this part of the strategy becomes of more importance. Philips can at that time change this part of the strategy, but as by that time the situation will have changed it is of no use to determine that part of the strategy at this time.

The last element of this strategy is the enforcement of Philips patents. As patents are used more as a defensive measure than as revenue opportunities, the choice to enforce a patent will also be of a defensive nature. This means that Philips should typically settle suits with cross-licensing agreements. The infringing company should also pay in such a settlement for the additional value of Philips portfolio over its portfolio.

The most important element of the complete strategy is that Philips closely follows the development of alliances, which standardize (elements of) DRM systems. It should then promote those standards that benefit Philips and prevent other standards from becoming dominant. Based on Philips' position amongst other patent holders this could very well result in an (industry) effort lead by Philips and one or more other consumer electronics companies (specifically Sony).

6.3 Strategy Summary and Additional Remarks

The implementation of a patent strategy requires the adaptation of such strategy to company requirements. These requirements include the necessity of a patent strategy to fit in a company's overall strategy alongside other strategies, such as a research strategy and patent strategies on other technologies. This paper does therefore not deliver a turnkey solution, but isolates management questions surrounding Philips DRM patent portfolio to grant proper attention to this valuable resource.

The strategy can be summarized as using a combined licensing and defensive strategy to ensure access to essential DRM patents. The most important elements in the strategy and the reason why they are important are:

- Monitoring the creation, changes within and output of alliances that standardize (elements of) DRM - because standardization is necessary to create interoperability and both access to such standards is essential as well as the dominance of a standard that Philips favors.
- Cooperating with other consumer electronics companies based on common goals - because neither Philips nor any other consumer electronics company can create or promote such a standard by itself.

A patent strategy covers all three fields of patenting, licensing and enforcement, and more specifically the relation between these fields. In this paper, it has been shown that patent strategy research truly differs from research that focuses on only one of these three fields of research. The relations between these fields are very important; we have seen for example that a lack of defensive patenting requires measures to be taken to ensure that licenses can be obtained.

Most importantly, this research paper provides a very basic method for determining a patent strategy. An important part of this method is the actual search for patents and the comparison of the patent portfolios. This requires both the technology that the portfolio covers and the companies that hold important patent portfolios to be analyzed. Determining a patent strategy is a matter of combining many different kinds of information from many different sources.

The very basic model that this paper provides can be elaborated upon in further research. As there is little existing research on patent strategies, it is not the goal of this paper to develop this model much further or test its results with case studies from the past. There is much more research that can be done on patent strategies. As these strategies are receiving more attention in innovation driven companies, it is very likely that such research will get the attention it deserves.

This research paper provides many suggestions for future research, but it would be best to start of such research by looking at actual uses of patent strategies. In other words, to determine what types of companies in which industries are actively planning their patenting, licensing and enforcement activities. How these companies gear these activities to one another and why they do so. Patent strategies are likely to be used more in certain industries (e.g. electronics) or for certain types of innovations (e.g. less so for incremental innovations).

Research is also needed on actual elements of strategies, such as what methods of defensive patenting companies use. In this paper, patent thickets and patent walls are mentioned. Other, related, terms that are sometimes used are patent minefields (many small patents to cover variations on an innovation), patent arrows (many patents on advances to a single implementation of an innovation) and omnibus patents (a single patent that is very broad and contains many claims). Likely, there are many more strategies and nuances in these strategies. A list should be made of all of these to be able to compare them and create a common terminology for patent strategy research.

Another interesting question for future research is what the importance of alliances between companies are in their patenting, licensing and enforcement behavior. As this case shows, alliances are an important part of patent strategies.

Finally, future research will have to deal with some of the same difficulties as this research paper. Most importantly, companies are very hesitant about sharing information regarding patenting, licensing and enforcement. Secondly, strategies for patent portfolios are highly dependent on the technology that the patents cover and other factors that are not directly patent related. The only way to overcome these difficulties is by performing the actual research. I hope that the increasing importance of patents will heighten interest in patent strategy research so that a better understanding is created of the importance of this type of research to the study of intellectual property in general.

References

Books, periodicals, publications and working papers

Arundel, Anthony (2001) "The relative effectiveness of patents and secrecy for appropriation", *Research Policy*, Vol. 30, pp 611-624.

Arundel, Anthony and Kabla, Isabelle (1998) "What percentage of innovations are patented? Empirical estimates for European firms", *Research Policy*, Vol 27, pp 27-141

Bessen, James (2003) "Patent Thickets. Strategic Patenting of Complex Technologies", Working Paper, October 2003, Research on Innovation. Available online at http.//www.researchoninnovation.org/thicket.pdf

Bosenblatt, Trippe and Mooney (2002), "Digital Rights Management Business and Technology", M&T books, New York.

Cockburn, Iain M.; Kortum, Samuel and Stern, Scott (2002) "ARE ALL PATENT EXAMINERS EQUAL? THE IMPACT OF CHARACTERISTICS ON PATENT STATISTICS AND LITIGATION OUTCOMES", Working Paper 8980, June 2002, National Bureau of Economic Research, Cambridge (MA) Available online at http://www.nber.org/papers/w8980

Cohen, Wesley M.; Nelson, Richard R.; and Walsh, John P (2000) "PROTECTING THEIR INTELLECTUAL ASSETS: APPROPRIABILITY CONDITIONS AND WHY U.S. MANUFACTURING FIRMS PATENT (OR NOT)", Working Paper (7552), February 2000, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w7552

Crampes, Claude and Langinier, Corinne (2002) "Litigation and settlement in patent infringement cases"; *The Rand Journal of Economics*, Summer 2002, Vol. 33, No. 2, ABI/INFORM Global, pg. 258 and further

Davis, Lee (2002) "THE STRATEGIC USE OF PATENTS IN INTERNATIONAL BUSINESS", Workshop Paper to be delivered to the 28th Annual EIBA Conference Athens, Greece, December 2002, Department of Industrial Economics and Strategy, Copenhagen Business School

Gallini, Nancy T. (1984) "Deterrence by Market Sharing: A Strategic Incentive for Licensing", *The American Economic Review*, Vol. 74, No. 5, December 1984, pp. 931-941.

Haitsma, J; Kalker, T; and Oostveen, J (2001) "Robust Audio Hashing for Content Identification", Content based multimedia Indexing (CBMI) 2001, Brescia Italy. Available online at http://www.extra.research.philips.com/natlab/download/audiofp/cbmi01audiohashv1.0.pdf

Hall, Bronwyn H. (1999) "INNOVATION AND MARKET VALUE", Working Paper 6984, February 1999, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w6984

Hall, Bronwyn H. and Ham, Rose Marie (1999) "THE PATENT PARADOX REVISITED: DETERMINANTS OF PATENTING IN THE US SEMICONDUCTOR INDUSTRY, 1980-94", Working Paper 7062, March 1999, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w7062

Hall, Bronwyn H., Jaffe, Adam and Trajtenberg, Manuel (2000) "MARKET VALUE AND PATENT CITATIONS: A FIRST LOOK", Working Paper 7741, June 2000, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w7741

Hall, Bronwyn H., Jaffe, Adam B and Trajtenberg, Manuel (2001) "THE NBER PATENT CITATIONS DATA FILE. LESSONS, INSIGHTS AND METHODOLOGICAL TOOLS", Working Paper 8498, October 2001, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w8498

Kauko, Karlo (2000) "The Microeconomics of Innovation. Oligopoly Theoretic Analyses with Application to Banking and Patenting", Ph.D. Thesis, Helsinki School of Economics and Business Administration, Helsinki (Finland)

Lanjouw, Jean O. and Lerner, Josh (1997)"THE ENFOREMCENT OF INTELLECTUAL PROPERTY RIGHTS: A SURVEY OF THE EMPIRICAL LITERATURE", Working Paper 6296, December 1997, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w6296

Lanjouw, Jean O. and Schankerman, Mark (2001) "ENFORCING INTELLECTUAL PROPERTY RIGHTS", Working Paper 8656, December 2001, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w8656

Lanjouw, Jean O., Pakes, Ariel and Putnam, Jonathan (1996) "HOW TO COUNT PATENTS AND VALUE INTELLECTUAL POROPERTY. USES OF PATENT RENEWAL AND APPLICATION DATA", Working Paper 5741, September 1996, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w5741

Lerner, Josh, Tirole, Jean and Strojwas, Marcin (2003) "COOPERATIVE MARKETING AGREEMENTS BETWEEN COMPETITORS: EVIDENCE FROM PATENT POOLS", Working Paper 9680, May 2003, National Bureau of Economic Research, Cambridge (MA). Available online at http://www.nber.org/papers/w9680

Lyon, Gordon E. (2002) "Information Technology: A Quick-Reference List of Organizations and Standards for Digital Rights Management", NIST Special Publication 500-241 (October 2002), National Institute of Standards and Technology, Technology Administration, US Department of Commerce, Maryland.

Mori R. and Tashiro, S. (1987) "The concept of Software Service System (SSS)", *Trans. IEICE (Institute of Electronics, Information and Communication Engineers)*, J70-D. 1, January 1987, pp. 70-81

Pakes, Ariel; and Temin, Peter (1991) "Patent Expiration, Entry, and Competition in the U.S. Pharmaceutical Industry. Comments and Discussion", *Brookings Papers on Economic Activity, Microeconomics*, Vol. 1991, pp. 49-66.

Rockett, Katharine E (1990) "Choosing the Competition and Patent Licensing", The Rand Journal of Economics, Spring 1990, Vol. 21, No. 1, ABI/INFORM Global, pg. 161 and further.

Somaya, Deepak (2002a) "Patent Litigation in the United States (1970-2000)", Working Paper, March 30, 2002, Robert H. Smith School of Business, University of Maryland (MD)

Somaya, Deepak (2002b) "Theoretical Perspectives on Patent Strategy", Working Paper, Robert H. Smith School of Business, University of Maryland, State Park (MD).

Stefik, M. (1996) "Letting Loose the Light: Igniting Commerce in Electronic Publication," in Mark Stefik (Ed.), Internet Dreams: Archetypes, Myths, and Metaphors. Cambridge, Mass: MIT Press, October 1996

Stern, Richard H. (2001) "Amazon's One-Click Patent Loses Its Teeth", *IEEE Micro Law*, Vol. 21, No. 2, March/April 2001.

Teece, David J. (2000) "Managing Intellectual Capital", Oxford University Press, New York.

Trajtenberg, Manuel (1990) "A Penny for Your Quotes: Patent Citations and the Value of Innovations", *The Rand Journal of Economics*, Spring 1990; Vol. 21, No. 1, ABI/INFORM Global, pg. 172 and further

Yoffie, David B; editor (1997) "COMPETING IN THE AGE OF DIGITAL CONVERGENCE", Harvard Business School, Boston.

Websites

4CEntity.com
http://www.4centity.com/tech/cprm
accessed on October 17th 2003

Canon.com
http://www.canon.com/about/business/index.html
accessed on October 17th 2003

ContentGuard.com
http://www.contentguard.com/about.asp
accessed on October 17th 2003

Digital-CP.com
www.digital-cp.com
accessed on October 17th 2003

DRM Watch, a
DRM Watch update newsletter, 26-02-2003
Available online at www.giantstepsmts.com/drmwatch.htm
accessed on October 17th 2003

DRM Watch, b
DRM Watch update newsletter, 10-04-2003
Available online at www.giantstepsmts.com/drmwatch.htm
accessed on October 17th 2003

DTCP.com
www.dtcp.com
accessed on October 17th 2003

DVB.org
www.dvb.org
accessed on October 17th 2003

Epa.org
Improved patent searching on the internet, Epidos news issue January 2000, April 17th 2000, European Patent Office, available online
http://www.european-patent-office.org/news/epidosnews/source/epd_1_00/14_1_00_e.htm
accessed on October 7th 2002

IBM.com
http://www.ibm.com/products/us/index.html
accessed on October 17th 2003

InterTrust.com, a
http://www.intertrust.com/main/overview/drm.html
accessed on 30-10-2002

InterTrust.com, b
http://www.intertrust.com/main/ip/patentportfolio.html
accessed on October 17th 2003

IPmall.info
Comparison between IPC and USPC, Hsin-Hsin Liu,
http://www.ipmall.info/hosted_resources/bp00/liu.htm
accessed on September 25th 2002

ISMA.tv
http://www.isma.tv/about/ourmembers
accessed on October 17th 2003

Key2Audio.com
http://www.key2audio.com/start/default.asp
accessed on November 6th 2002

Microsoft.com, a
http://www.microsoft.com/windows/windowsmedia/WM7/DRM/definition.asp
accessed on September 6th 2002

Midbartech.com
http://www.midbartech.com/
accessed on November 6th 2002

SDMI.org
www.sdmi.org/participant_list.htm
accessed on October 17th 2003

TV-Anytime.org
www.tv-anytime.org
accessed on October 17th 2003

Whatis.com
http://whatis.com search for "XRML"
accessed on November 6th 2002

W3.org, a
Presentation at the W3C DRM Workshop (Sophia Antipolis, France 22-23 January 2001) by Dr. Renato Iannella (Chief Scientist of IPR Systems Pty Ltd). Available online at
http://www.w3.org/2000/12/drm-ws/pp/iprsystems-iannella2.pdf
accessed on September 6th 2002

Wipo.int, a
Introductory manual to the IPC, chapter 2, published online,
http://www wipo.int/classifications/en/ipc/manual/manual2.htm
accessed on September 23rd 2002

Wipo.org
THE FIRST TWENTY-FIVE YEARS OF THE INTERNATIONAL PATENT CLASSIFICATION (IPC), published online to commemorate the anniversary of the IPC classification,
http://www.wipo.org/classifications/en/ipc/ipc_25/preface.htm
accessed on September 23rd 2002

SealedMedia.com
http://www.sealedmedia.com/company/default.asp
accessed on October 12th 2003

Xanadu.com
http://www.xanadu.com/tco/index.html
accessed on September 6th 2002

APPENDIXES

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A - Searching for DRM Patents

Summary:

After a first search, the **Query 1** is formed as:
((Right*1 ADJ management) OR (superdistribution OR (super ADJ distribution))

Add to **Query 1** to make **Query 2:**
Usage ADJ right*1
Rights*1 ADJ enforcement
License ADJ control
Rights ADJ protection
(((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management)
InterTrust
Contentguard
Digital ADJ object ADJ identifier
Digital ADJ property ADJ rights ADJ language
Rights ADJ language
Rights ADJ grammar
Content ADJ rights
(Content ADJ usage) AND (usage ADJ management)
(Copy ADJ protection) AND (content ADJ management)

Query 2:
((usage ADJ transactions) OR Contentguard OR InterTrust OR (Right*1 ADJ enforcement) OR (Content ADJ rights) OR ((Electronic or digital) ADJ content*1 ADJ right*1) OR ((Content ADJ usage) AND (usage ADJ management)) OR (Protection ADJ digital ADJ works) OR (Right*1 ADJ (language OR grammar)) OR (((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management) OR (Digital ADJ object ADJ identifier) OR ((Electronic OR digital) ADJ rights ADJ protection) OR ((Content ADJ management) AND (copy ADJ protection))) OR (right*1 ADJ management) OR (superdistribution) OR ((super) ADJ distribution)

Remove from **Query 2** to make **Query 3:**
Digital ADJ object ADJ identifier

Add to **Query 2** to make **Query 3:**
Content ADJ protection ADJ2 media
Copyright ADJ control
(Copy OR display OR edit OR rendering) ADJ rights
Usage ADJ right*1
(Copies OR copying) ADJ allowed
((Copy OR copyright OR content) ADJ protection) WITH (ticket OR watermark OR fingerprint)
Copy ADJ protected ADJ content
(Encrypt*3 ADJ content) AND (copy ADJ protection)

Query 3:
((usage ADJ transactions) OR Contentguard OR InterTrust OR (Right*1 ADJ enforcement) OR (Content ADJ rights) OR ((Electronic OR digital) ADJ content*1 ADJ right*1) OR ((Content ADJ usage) AND (usage ADJ management)) OR (Protection ADJ digital ADJ works) OR (Right*1 ADJ (language OR grammar)) OR (((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management) OR ((Electronic OR digital) ADJ rights ADJ protection) OR ((Content ADJ management) AND (copy ADJ protection))) OR (right*1 ADJ management) OR (superdistribution) OR ((super) ADJ distribution) OR (Content ADJ protection ADJ2 media) OR (Copyright ADJ control) OR ((Copy OR display OR edit OR rendering) ADJ rights) OR (Usage ADJ right*1) OR ((Copies OR copying) ADJ allowed) OR (((Copy OR copyright OR content) ADJ protection) WITH (ticket OR watermark OR fingerprint)) OR (Copy ADJ protected ADJ content) OR ((Encrypt*3 ADJ content) AND (copy ADJ protection))
The results of the Query 3 (in Micropatent, 1 per family) are exported to Questel/Orbit where they are filtered on ECLA if this has been assigned, else IPC (see Appendix B). The Philips patents in these results are then manually reviewed.

The rest of this appendix explains the process of formulating the queries in more detail.

Step 1: Formulating **Query 1**[72]

To formulate Query 1 we start of with the following first query (this is not our final choice for Query 1):
(((right*1 OR content OR product) ADJ management) OR DRM OR ((license OR content) ADJ server) OR (royalt*3 ADJ (payment OR transfer)) OR (superdistribution OR (super ADJ distribution)))

After manual review of some of the patents in the result set, the following parts of the query are removed:
Content ADJ management
Product ADJ management
DRM
License ADJ server
Content ADJ server
Royalt*3 ADJ (payment OR transfer)

Right*1 ADJ management
693
Limited to USPC / IPC[73]: 670

Electronic ADJ product ADJ management
1
Limited to USPC / IPC: 0

Digital ADJ product ADJ management
0
Limited to USPC / IPC: 0

Superdistribution OR (super ADJ distribution)
96
Limited to USPC / IPC: 92
There's an overlap of 32 patents in the results of this query and the (Right*1 ADJ management) query.
(Right*1 ADJ management) AND (Superdistribution OR (super ADJ distribution))
32

Query 1 becomes ((Right*1 ADJ management) OR (superdistribution OR (super ADJ distribution))

[72] Queries in Micropatent on 14-10-2002
[73] Limited to USPC / IPC means limited to classes: 380 OR 705 OR 707 OR 709 OR 713 OR 725 OR G06 OR G11 OR H04

Step 2: Formulating **Query 2**

For each query the number of results that overlap with the results of query 1 (indicated as AND DRM) and the number of results that do not overlap with query 1 (indicated as NOT DRM) are given.

Part A[74]

Usage ADJ right*1
AND DRM: 89 hits
NOT DRM. 298 hits

Right*1 ADJ use
AND DRM: 93 hits
NOT DRM: 2608 hits

Right*1 enforcement
AND DRM: 21 hits
NOT DRM. 22 hits

Controlled ADJ distribution
AND DRM 11 hits
NOT DRM 1947 hits

Secure ADJ distribution
AND DRM 47 hits
NOT DRM 372 hits

Content ADJ distribution
AND DRM 170 hits
NOT DRM 2029 hits

Trust*2 ADJ distribution
AND DRM 0
NOT DRM 20

Controlling ADJ distribution
AND DRM 43 hits
NOT DRM 3459

Key ADJ distribution
AND DRM 40
NOT DRM 1449

Right*1 ADJ distribution
AND DRM 16 patents
NOT DRM 227 patents

[74] Queries in Micropatent between 15-10-2002 and 20-10-2002

Trust
AND DRM 115 hits
NOT DRM 6455 hits

Trust*2 ADJ environment
AND DRM 27
NOT DRM 126

Trust*2 ADJ system
AND DRM 26
NOT DRM 369

Trust*2 ADJ client
AND DRM 3
NOT DRM 87

Trusted ADJ computing
AND DRM 7
NOT DRM 178

Distributed ADJ trust
AND DRM 2
NOT DRM 17

"Protection digital works"
AND DRM 3
NOT DRM 4

Right*1 ADJ (language OR grammar)
AND DRM 20
NOT DRM 55

(Render OR Transport OR (Derivative ADJ work)) ADJ rights
AND DRM 7
NOT DRM 3

Pay ADJ per ADJ (view OR listen)
AND DRM 96
NOT DRM 4013

License ADJ management
AND DRM 18
NOT DRM 241

Content ADJ management
AND DRM 77
NOT DRM 1165

Access ADJ management
AND DRM 37
NOT DRM 1818

Conditional ADJ access
AND DRM 32
NOT DRM 2131

License ADJ control
AND DRM 24
NOT DRM 69

(Electronic OR digital) ADJ voucher
AND DRM 2
NOT DRM 65

(Electronic OR digital) ADJ rights ADJ protection
AND DRM 25
NOT DRM 31

Rights ADJ protection
AND DRM 58
NOT DRM 67

Product ADJ management
AND DRM 4
NOT DRM 466

(Product ADJ management) AND ((license OR content) ADJ server)
AND DRM 0
NOT DRM 3
None seem relevant

Copyright ADJ management
AND DRM 38
NOT DRM 268

(((Intellectual ADJ property) OR (Intellectual ADJ property ADJ right*1)) ADJ management)
AND DRM 29
NOT DRM 44

Transaction ADJ management
AND DRM 37
NOT DRM 1134

Specify ADJ use
AND DRM 4
NOT DRM 611
Few seem relevant, limiting the results to USPC / IPC classes 380 OR 705 OR 707 OR 709 OR 713 OR 725 OR G06 OR G11 OR H04.
NOT DRM 341
Still few seem relevant

InterTrust

AND DRM 77

NOT DRM 8

Contentguard

AND DRM 4

NOT DRM 3

XRML

AND DRM 10

NOT DRM 1

Returns too many irrelevant results (abbreviation)

Extensible ADJ rights ADJ markup ADJ language

ADN DRM 0

NOT DRM 1

Does not seem relevant

To find patents mentioning: Information and Content Exchange (ICE):

Information ADJ content ADJ exchange

AND DRM 0

NOT DRM 35

Digital ADJ object ADJ identifier

AND DRM 29

NOT DRM 21

Digital ADJ property ADJ rights ADJ language:

AND DRM 6

NOT DRM 2

DPRL returns too many irrelevant results (abbreviation)

Stefik

AND DRM 17

NOT DRM 109

Although some seem relevant, many deal with other technologies. Some mentions of Stefik refer to a different person than Mark Stefik of Xerox PARC.

Searching for "Stefik" in the inventor field

AND DRM 3

NOT DRM 28

Most patents registered with Stefik as inventor deal with DRM, but this is of course not a method usable to find Philips patents.

Searching for "Stefik" in non-patent citations returns more results, but the relevant results are the same as in the previous query (Stefik as inventor).

"Letting loose light" ("the" is left out as this is a word Micropatent does not search for)
AND DRM 0
NOT DRM 1

"Igniting commerce in electronic publication"
Same results as above in "Letting loose the light"

Searching for Mori AND/ OR Tashiro results in far too many irrelevant results (many people share this name)

Software service system
NOT DRM 14
AND DRM 2

controlling ADJ dissemination
AND DRM 1
NOT DRM 37
Few seem relevant

Right*1 ADJ language
AND DRM 16
NOT DRM 46
Some occurrences of "right" at the end of one sentence and "language" at the beginning of the next sentence

Rights ADJ language
AND DRM 16
NOT DRM 28
Many seem relevant

Rights ADJ grammar
AND DRM 11
NOT DRM 17
Many seem relevant

((rights ADJ grammar) AND (rights ADJ language))
AND DRM 7
NOT DRM 16
It seems many that mention both grammar and language.

(conditional ADJ access) AND ((right ADJ play) OR (right ADJ copy) OR (right ADJ distribute) OR (usage ADJ right) OR (right ADJ use))
54 patents
AND DRM 3
NOT DRM 51

Content*1 ADJ right*1
AND DRM 111
NOT DRM 760
Few seem relevant

Content ADJ rights
AND DRM 82
NOT DRM 48

(electronic OR digital) ADJ content*1 ADJ right*1
AND DRM 23
NOT DRM 5

Access ADJ management
AND DRM 37
NOT DRM 1818

Access ADJ rights
AND DRM 174
NOT DRM 4292

Content ADJ management
AND DRM 77
NOT DRM 1165

(Electronic OR digital) ADJ ticket*1
AND DRM 6
NOT DRM 479

Usage ADJ control
AND DRM 52
NOT DRM 657

Control ADJ use
AND DRM 44
NOT DRM 13563

Specify ADJ content ADJ use
AND DRM 0
NOT DRM 0

Right ADJ specify ADJ use
AND DRM 0
NOT DRM 0

Charge ADJ per ADJ use
AND DRM 0
NOT DRM 42

Usage ADJ metering
AND DRM 27
NOT DRM 174

Usage ADJ management
AND DRM 14
NOT DRM 160

Content ADJ usage
AND DRM 82
NOT DRM 329

Content ADJ usage ADJ management
AND DRM 5
NOT DRM 1

(content ADJ usage) AND (usage ADJ management)
AND DRM 14
NOT DRM 23

Prevent*3 ADJ unauthorized ADJ use
AND DRM 46
NOT DRM 2606

(prevent*3 ADJ unauthorized ADJ use) AND content
AND DRM 42
NOT DRM 527

(Secure OR (secure ADJ electronic) OR (secure ADJ electronic ADJ content) OR (secure ADJ content)) ADJ distribution
AND DRM 63
NOT DRM 418

Part B[75]

Controlling ADJ use
AND DRM 30
NOT DRM 1579

Rights ADJ voucher
AND DRM 0
NOT DRM 0

Regulate ADJ distribution
AND DRM 0
NOT DRM 248

Regulate ADJ copying
AND DRM 1
NOT DRM 5

Limiting ADJ usage
AND DRM 4
NOT DRM 163

[75] Queries in Micropatent between 21-10-2002 and 25-11-2002

Limiting ADJ use
AND DRM 22
NOT DRM 4298

Limiting ADJ copying
AND DRM 0
NOT DRM 36

Limit ADJ copying
AND DRM 6
NOT DRM 80

Piracy
AND DRM 125
NOT DRM 1576

Usage ADJ transactions
AND DRM 3
NOT DRM 44

(Conditional ADJ access) AND (right ADJ copy)
AND DRM 1
NOT DRM 27

(Conditional ADJ access) AND (right ADJ distribute)
AND DRM 1
NOT DRM 5

(Conditional ADJ access) AND (derivative ADJ right)
AND DRM 0
NOT DRM 0

ECM OR EMM
AND DRM 30
NOT DRM 8017

Authorized ADJ domain
AND DRM 151
NOT DRM 6357

Compliance ADJ management
AND DRM 2
NOT DRM 55

License ADJ facility
AND DRM 2
NOT DRM 1

(Content ADJ management) AND (copy ADJ protection)
AND DRM 23
NOT DRM 37

Software ADJ service ADJ system
AND DRM 2
NOT DRM 10

For the queries of part A and B that would seem relevant after performing these queries, a manual check is done to verify whether these patents are or aren't DRM related. Only the patents that do not overlap with Query 1 are reviewed (title and abstract)

Right*1 ADJ enforcement
MANY

Content ADJ rights
SOME

(Electronic or digital) ADJ content*1 ADJ right*1
MANY

(Content ADJ usage) AND (usage ADJ management)
MANY

Protection ADJ digital ADJ works
FEW

Right*1 ADJ (language OR grammar)
SOME

((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management
SOME

Digital ADJ object ADJ identifier
SOME

(Electronic OR digital) ADJ rights ADJ protection
MANY

(Content ADJ management) AND (copy ADJ protection)
MANY

License ADJ facility
NONE

Compliance ADJ management
NONE

usage ADJ transactions
MANY

Software service system
NONE

Contentguard
MANY

InterTrust
SOME

(Product ADJ management) AND ((license OR content) ADJ server)
NONE

License ADJ control
SOME, but check whether they are already in the results of another query

(Render OR Transport OR (Derivative ADJ work)) ADJ rights
NONE

Query 2 is then formulated as:

((usage ADJ transactions) OR Contentguard OR InterTrust OR (Right*1 ADJ enforcement) OR (Content ADJ rights) OR ((Electronic or digital) ADJ content*1 ADJ right*1) OR ((Content ADJ usage) AND (usage ADJ management)) OR (Protection ADJ digital ADJ works) OR (Right*1 ADJ (language OR grammar)) OR (((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management) OR (Digital ADJ object ADJ identifier) OR ((Electronic OR digital) ADJ rights ADJ protection) OR ((Content ADJ management) AND (copy ADJ protection))) OR (right*1 ADJ management) OR (superdistribution) OR ((super) ADJ distribution)

969 results, 21 of these with assignee: philips OR cryptoworks OR cryptoworx (there's one patent with cryptoworx as assignee)

1 per family:
14 patents

Part 3: Formulating **Query 3**

As some Philips DRM patents are not found using only **Query 2**, this query needs to be changed.
Some searches have been limited to a number of IPC classes, these classes are:
G06F00100 OR G06F00946 OR G06F01214 OR G06F017 OR G11B00390 OR G11B02000 OR H04L00900 OR H04L00930 OR H04L00932 OR H04L01214 OR H04L02906 OR H04N00716* OR H04N01717* OR H04N007 OR H04N005913

Secure*1 ADJ domain
62
Few seem relevant

Authorized ADJ domain
20
Few seem relevant

(Domain ADJ based)
1281
Few seem relevant

Domainbased
6
Few seem relevant (exactly the same patents as in the query above, "authorized ADJ domain")

Usage ADJ conditions
2261
Limited to IPC: 110
Few seem relevant

Conditions NEAR1 (use OR usage)
47156
Few seem relevant

(Copy OR copying) ADJ control (= copy control information (CCI))
2692 hits

Copy ADJ control ADJ information
400
Some seem relevant

Content ADJ protection ADJ2 media (= copy protection for prerecorded / Recordable media (CPPM/CPRM))
19
Many seem relevant

Content ADJ protection
400
Limited to IPC: 246 hits, of which 159 not in Query 2 of "content ADJ protection ADJ2 media"
Few seem relevant

Copy ADJ protection ADJ2 media
41
Few seem relevant

Copyright ADJ protection
9578
Limited to IPC: 2557
Limited to ECLA: 68 hits
In these 68 hits some seem relevant
Pirated AND content
283
Few seem relevant

Illicit ADJ content
10
Almost all are Philips patents

Copy ADJ1 management (= copy (generation) management)
656 hits
Most are technical implementations not relevant to this search

Copy ADJ generation ADJ management
228 hits
140 hits limited by IPC (only a few DRM patents seem to be left out this way)
Few relevant to DRM

Serial ADJ copy ADJ management
351
Some seem relevant (more than in copy generation management)

(Protection OR use) ADJ (digital OR electronic) ADJ (works OR content OR media)
390
271 not in Query 2
Some seem relevant

Content ADJ (protection OR screening)
548
Few seem relevant

(Secure ADJ (electronic OR digital) ADJ distribution) OR (secure ADJ content ADJ distribution) OR (secure ADJ (electronic OR digital) ADJ content ADJ distribution)
91
40 not in Query 2
Some seem relevant

(Right ADJ decode) OR (decode ADJ right*1)
47
41 not in Query 2
None seem relevant

Content ADJ management ADJ information
115
Few seem relevant

(Duplication OR reproduction OR copy OR copyright) ADJ control
5652 hits

(Duplication OR reproduction) ADJ control
3663

Copy ADJ control
1979

Copyright ADJ control
109
100 not in Query 2
Many seem relevant

Copyright ADJ management
334
Limited to IPC: 181 of which 132 are not in Query 2
Few seem relevant

Secured ADJ content
327 hits
Limited to IPC: 206 of which 120 are not in Query 2
Few seem relevant

(Usage OR access) ADJ (right*1 OR rule*1)
8243

Asset ADJ management
950
Limited to IPC: 470
Few seem relevant: this query finds mostly financial systems

Copy ADJ protected
841
Limited to IPC: 453 of which 436 not in Query 2
Some seem relevant

Protect*3 NEAR1 media
1674
Limited to IPC: 152 of which 129 not in Query 2
Some seem relevant

Intellectual ADJ property ADJ right*1
612
Limited to IPC. 303 of which 234 not in Query 2
Few seem relevant

Ticket
Limited to IPC. 4040
Copy and ticket, Limited to IPC: 1135
((Copy OR copyright) ADJ protection) AND ticket, Limited to IPC: 188 of which 147 not in Query 2
Some seem relevant

Watermark
Limited to IPC: 1640
Copy AND watermark, Limited to IPC: 942
((Copy OR copyright) ADJ protection) AND watermark, Limited to IPC: 391 of which 323 not in Query 2
Some seem relevant

Fingerprint
Limited to IPC. 2448
Copy AND fingerprint, Limited to IPC: 1033

((Copy OR copyright) ADJ protection) AND fingerprint, Limited to IPC: 197 of which 147 not in Query 2
Few seem relevant -> change search to "(digital OR electronic) ADJ fingerprint"
((Digital OR electronic) ADJ fingerprint) AND ((Copy OR copyright) ADJ protection) 27 hits, of which 16 not in Query 2
Some seem relevant, but these seem to be found in other result sets as well

Hash
Limited to IPC: 5871
Copy AND hash, Limited to IPC: 2702
((Copy OR copyright) ADJ protection) AND hash, Limited to IPC: 571 of which 460 not in Query 2
Some seem relevant, but these seem to be found in other result sets as well.

Management AND watermark
Limited to IPC: 621 of which 473 not in Query 2
Few seem relevant

Watermark WITH management
339 hits
Limited to IPC: 183 of which 128 not in Query 2
Some seem relevant, but these seem to be found in other result sets as well.

Rule*1 WITH (content OR media OR work)
22558 hits

Content ADJ usage
Limited to IPC: 1548

Access ADJ right*1
Limited to IPC: 2474

License WITH content
Limited to IPC: 535 of which 369 not in Query 2
Few seem relevant

Licens*3 ADJ content
212
109 not in Query 2
Some seem relevant

Copy ADJ once
316 hits
Limited to IPC: 139 of which 130 not in Query 2
Some seem relevant

Copy ADJ never
119, of which 53 not in the result set of "copy once"
Some of these still seem relevant

(Copy OR display OR edit OR rendering) ADJ rights
110 hits
Limited to IPC. 82 of which 77 not in Query 2
Many seem relevant

Rights ADJ enabled
11 hits
Limited to IPC: 6
Some seem relevant

Revocation
1191 hits
Limited to IPC: 770
Few seem relevant

Usage ADJ right*1
413
Limited to IPC: 210 of which 205 not in Query 2
Many seem relevant

Key ADJ management
2689 hits
Limited to IPC: 1419
Few seem relevant

(Key ADJ management) AND content
Limited to IPC: 660 of which 559 not in Query 2
Few seem relevant

Key ADJ distribution
1565
Limited to IPC: 898
Few seem relevant

(Key ADJ distribution) AND content
556
Limited to IPC: 369
Some seem relevant

Conditional ADJ use
57 hits
Limited to IPC: 16 of which 15 not in Query 2
None seem relevant

Digital ADJ content
1835 hits
Limited to IPC: 1052 of which 805 not in Query 2
Few seem relevant

Copyright ADJ information
1327
Limited to IPC: 638 of which 583 not in Query 2
Some seem relevant, but these seem to be found in other result sets as well

Copyright WITH information
164539
Limited to IPC: 10265
Copyright ADJ detection
69
Limited to IPC 15 of which 15 not in Query 2
Few seem relevant: most are focused on watermarking on an implementation level

Copyright WITH detection
118184
Limited to IPC: 2896

Copyright NEAR4 detection
4422
Limited to IPC: 128 of which 126 not in Query 2
Few seem relevant

Limit ADJ copying
96 hits
Limited to IPC: 35 of which 19 not in Query 2
None seem relevant

(Copies OR copying) ADJ allowed
284
Limited to IPC: 122 of which 94 not in Query 2
Many seem relevant

(Unauthorized OR unauthorised) ADJ copy*3
2172
Limited to IPC: 1180 of which 1016 not in Query 2
Few seem relevant

((Copy OR copyright OR content) ADJ protection) WITH (ticket OR watermark OR fingerprint)
375
Limited to IPC: 222 of which 208 not in Query 2
Many seem relevant

These next four queries are very much focused on Philips (phrases used in Philips):

Conforming ADJ devices
48
Limited to IPC: 7 of which 7 not in Query 2
Only relevant ones are Philips patents that are also part of the result set of most other relevant queries

Compliant ADJ devices
634
Limited to IPC: 113 of which 104 not in Query 2
Some are relevant, but again mostly Philips patents that are also part of the result set of most other relevant queries

Compliant ADJ world
14
Limited to IPC: 10 of which 10 not in Query 2
Only 2 seem relevant and these are again Philips patents that are also part of the result set of most other relevant queries

Copy ADJ protected ADJ content
69
Limited to IPC: 57 of which 55 not in Query 2
Most seem important, but almost all are Philips patents!

Control WITH content
129023 hits
Limited to IPC: 9415

playback ADJ only
880
Limited to IPC: 120 of which 104 not in Query 2
Few seem relevant

copy*3 ADJ allowed
330
Limited to IPC: 140 of which 128 not in Query 2
Some seem relevant

generation WITH copy
5771
Limited to IPC: 1091 of which 1035 not in Query 2
Few seem relevant

prevent*3 WITH copy*3
31011
Limited to IPC: 3328

(prevent*3 ADJ copy*3) OR (copy*3 ADJ prevent*3)
3494
Limited to IPC: 861 of which 811 not in Query 2
Few seem relevant

License ADJ management
272 hits
Limited to IPC: 204 of which 168 not in Query 2
Few seem relevant

Secure*1 WITH (content ADJ distribution)
165
Limited to IPC. 128 of which 41 not in Query 2
Some seem relevant, but these seem to be found in other result sets as well.

Watermark WITH ((copy OR copyright) ADJ protection)
324 hits
Limited to IPC: 193 of which 182 not in Query 2
Many seem relevant

Electronic ADJ publishing ADJ resources
7
Limited to IPC: 3
None seem relevant

(Copy ADJ protection) AND certificate
270
Limited to IPC: 209 of which 121 not in Query 2
Many seem relevant

Keywords / phrases specifically from Philips patents:

Complete ADJ data ADJ set
618
Limited to IPC: 83 of which 82 not in Query 2
The only DRM patents in this are Philips patents

Illicit ADJ reproduction
43
Limited to IPC: 17 of which 17 not in Query 2
Almost all are Philips patents

Content WITH (meta ADJ data)
664
Limited to IPC: 391 of which 309 not in Query 2
Few seem relevant

Replay ADJ attack
340
Limited to IPC: 226 of which 209 not in Query 2
Few seem relevant

Content ADJ key
1006
Limited to IPC: 509 of which 397 not in Query 2
Few seem relevant

Encrypt*3 ADJ content
1012
Limited to IPC: 781 of which 570 not in Query 2
Some seem relevant

(Encrypt*3 ADJ content) AND (copy ADJ protection)
189
Limited to IPC: 158 of which 87 not in Query 2
Many seem relevant

Encrypted ADJ content
815
Limited to IPC: 650 of which 460 not in Query 2
Some seem relevant

Watermark AND ticket AND (copy ADJ protection)
64
Limited to IPC: 46 of which 40 not in Query 2
Almost all are Philips patents

Content ADJ extension
69
Limited to IPC: 22 of which 22 not in Query 2
Few seem relevant

((copy OR copyright OR content) ADJ protection) AND complian*2
1344
Limited to IPC. 613 of which 518 not in Query 2
Some seem relevant

((Copy OR copyright OR content) ADJ protection) WITH complian*2
113
Limited to IPC: 91 of which 87 not in Query 2
Some seem relevant

((Copy OR copyright OR content) ADJ protection) AND certificate
597
Limited to IPC: 433 of which 304 not in Query 2
Some seem relevant

((Copy OR copyright OR content) ADJ protection) WITH certificate
42
Limited to IPC: 29 of which 28 not in Query 2
Some seem relevant

((Copy OR copyright OR content) ADJ protection) AND wobble
207
Limited to IPC: of which 80 not in Query 2

((Copy OR copyright OR content) ADJ protection) WITH wobble
38
Limited to IPC: 23 of which 23 not in Query 2
Many seem relevant, but many are Philips patents!

(Content OR audio OR video) ADJ authentication
130

Limited to IPC: 82 of which 65 not in Query 2
Few seem relevant

Secure ADJ digital ADJ music ADJ initiative
144
Limited to IPC. 92 of which 63 not in Query 2
Many seem relevant, but most are Philips

Query 3 is then chosen:

Remove from **Query 2**:
Digital ADJ object ADJ identifier

Add to **Query 2**.
Content ADJ protection ADJ2 media
Copyright ADJ control
(Copy OR display OR edit OR rendering) ADJ rights
Usage ADJ right*1
(Copies OR copying) ADJ allowed
((Copy OR copyright OR content) ADJ protection) WITH (ticket OR watermark OR fingerprint)
Copy ADJ protected ADJ content
(Encrypt*3 ADJ content) AND (copy ADJ protection)

Query 3:
((usage ADJ transactions) OR Contentguard OR InterTrust OR (Right*1 ADJ enforcement) OR (Content ADJ rights) OR ((Electronic OR digital) ADJ content*1 ADJ right*1) OR ((Content ADJ usage) AND (usage ADJ management)) OR (Protection ADJ digital ADJ works) OR (Right*1 ADJ (language OR grammar)) OR (((Intellectual ADJ property) OR (intellectual ADJ property ADJ right*1)) ADJ management) OR ((Electronic OR digital) ADJ rights ADJ protection) OR ((Content ADJ management) AND (copy ADJ protection))) OR (right*1 ADJ management) OR (superdistribution) OR ((super) ADJ distribution) OR (Content ADJ protection ADJ2 media) OR (Copyright ADJ control) OR ((Copy OR display OR edit OR rendering) ADJ rights) OR (Usage ADJ right*1) OR ((Copies OR copying) ADJ allowed) OR (((Copy OR copyright OR content) ADJ protection) WITH (ticket OR watermark OR fingerprint)) OR (Copy ADJ protected ADJ content) OR ((Encrypt*3 ADJ content) AND (copy ADJ protection))

12-05-2002
Query 3:
2255
Limited to 1 per family: 1406
Limited to IPC: 1295
Limited to IPC and 1 per family: 853

Query 3 AND Assignee: Philips OR Cryptoworks OR cryptoworx
124 (of which 2 are not yet in the Questel database, which are therefore removed)
Limited to 1 per family: 74
Limited to IPC: 106
Limited to IPC and 1 per family: 65

IPC	++ ECLA	Description
G06F 1/00 N7R1 seems most important	N7R1	G PHYSICS G06 COMPUTING; CALCULATING; COUNTING G06F ELECTRICAL DIGITAL DATA PROCESSING G06F1 Details of data-processing equipment not covered by groups G06F3/00 to G06F13/00 N Protection against unauthorised activity relating to computers and software 7 by manipulation of programmes or processes R to restrict resource availability, e.g. access to programmes or data 1 based on rights or privileges
	N7R2	2 by controlling access to software, e.g. licensing, vending or distribution
	N7A	A via auditing or logging data
	N5A(2C)	A by authenticating the identity of a user, process or remote node, e.g. using passwords 2 in co-operation with additional information C supplied by a third party, e.g. a certificate or counter-signature
G06F 9/46	R4	G PHYSICS G06 COMPUTING; CALCULATING; COUNTING G06F ELECTRICAL DIGITAL DATA PROCESSING G06F9 Arrangements for programme control, e.g. control unit G06F9/06 using stored programme, i.e. using internal store of processing equipment to receive and retain programme G06F9/46 Multiprogramming arrangements, e.g. using interrupt; Priority circuits therefor R Task interaction 4 Specific access rights for resources, e.g. using capability register
G06F12/14		G PHYSICS G06 COMPUTING; CALCULATING; COUNTING G06F ELECTRICAL DIGITAL DATA PROCESSING G06F12 Accessing, addressing or allocating within memory systems or architectures G06F12/14 . Protection against unauthorized use of memory
G06F17/60		G PHYSICS G06 COMPUTING; CALCULATING; COUNTING G06F ELECTRICAL DIGITAL DATA PROCESSING G06F17 Digital computing or data processing equipment or methods, specially adapted for specific functions G06F17/60 Administrative, commercial, managerial, supervisory or forecasting purposes

G11B 3/90		G PHYSICS G11 INFORMATION STORAGE G11B INFORMATION STORAGE BASED ON RELATIVE MOVEMENT BETWEEN RECORD CARRIER AND TRANSDUCER G11B3 Recording by mechanical cutting, deforming or pressing, e.g. of grooves or pits, Reproducing by mechanical sensing; Record carriers therefor G11B11/00 [N: and G11B13/00] take precedence; recording by cutting or deforming using laser beam G11B7/00, using electron beam G11B9/10) G11B3/68 . Record carriers G11B3/90 . . with means indicating prior or unauthorized use
G11B 20/00	P	G PHYSICS G11 INFORMATION STORAGE G11B INFORMATION STORAGE BASED ON RELATIVE MOVEMENT BETWEEN RECORD CARRIER AND TRANSDUCER G11B20 Signal processing not specific to the method of recording or reproducing; Circuits therefor G11B20/00P Circuits for prevention of unauthorized reproduction or copying, e.g. piracy
G11B 23/28		G PHYSICS G11 INFORMATION STORAGE G11B INFORMATION STORAGE BASED ON RELATIVE MOVEMENT BETWEEN RECORD CARRIER AND TRANSDUCER G11B23 Record carriers not specific to the method of recording or reproducing, Accessories, e.g. containers, specially adapted for co-operation with the recording or reproducing apparatus G11B23/28 Indicating or preventing prior or unauthorized use
G11C 16/22		G PHYSICS G11 INFORMATION STORAGE G11C STATIC STORES G11C16 Erasable programmable read-only memories G11C16/02 electrically programmable G11C16/06 . . Auxiliary circuits, e.g. for writing into memory G11C16/22 . Safety or protection circuits preventing unauthorised or accidental access to memory cells
H04L 9/00		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04L TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION H04L9 Arrangements for secret or secure communication

H04L 9/30		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04L TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION H04L9 Arrangements for secret or secure communication H04L9/28 . using particular encryption algorithm H04L9/30 . . Public key, i.e. encryption algorithm being computationally infeasible to invert and users' encryption keys not requiring secrecy
H04L 9/32		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04L TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION H04L9 Arrangements for secret or secure communication H04L9/32 . including means for verifying the identity or authority of a user of the system
H04L 12/14		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04L TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION H04L12 Data switching networks H04L12/02 . Details H04L12/14 . . Charging arrangements
H04L 29/06	B	H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04L TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION H04L29 Arrangements, apparatus, circuits or systems, not covered by a single one of groups H04L1/00 to H04L27/00 H04L29/02 . Communication control H04L29/06 . . ◎raveling◎zed by a protocol H04L29/06B . . Protocol definition or specification
	C6B	H04L29/06C . . . Protocols ◎raveling◎zed by their application H04L29/06C6 . . . . Protocols or architecture for network security H04L29/06C6B . . . . . for the confidentiality of the information ◎raveling over the network, e.g. encryption of data
	C6C	for allowing a denying access to network elements
	C6E	Maintaining multiple levels of security, e.g. classes, user profiles, policies
	C6G	for guaranteeing the integrity of the information, e.g. digital signatures
H04N 7/16		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04N PICTORIAL COMMUNICATION, e.g. TELEVISION H04N7 Television systems H04N7/16 . Secrecy systems; Subscription systems

H04N 7/03		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04N PICTORIAL COMMUNICATION, e.g. TELEVISION H04N7 Television systems H04N7/025 . Systems for the transmission of digital non-picture data, e.g. of text during the active part of a television frame H04N7/03 . . Subscription systems therefor
H04N 7/24	C12P	H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04N PICTORIAL COMMUNICATION, e.g. TELEVISION H04N7 Television systems H04N7/24 . Systems for the transmission of television signals using pulse code modulation H04N7/24C . . Bitstream control arrangements H04N7/24C12 . . . involving the control of media objects H04N7/24C12P . . . . Intellectual Property Rights management and protection therefor
H04N 5/913		H ELECTRICITY H04 ELECTRIC COMMUNICATION TECHNIQUE H04N PICTORIAL COMMUNICATION, e.g. TELEVISION H04N5 Details of television systems H04N5/76 . Television signal recording H04N5/91 . Television signal processing therefor H04N5/913 . . . for scrambling, for copy protection

Filtering the results of Query 1 to verify choice of classes:

G06F00100
G06F001 no more relevant results than a search for G06F00100

G06F00946
No DRM patents in G06F00906 that aren't also in G06G00946

G06F01214
G06F012 checked as well and no need to include

G06F01760
G06F017 seems to include DRM patents as well. For IPC use G06F017 and for ECLA use G06F01760.

G11B00390
Few patents seem related to DRM at first sight, but this class is very specific and is included any way.

G11B02000
No more results in G11B020 than in G11B02000

G11B023028
No patents seem to deal with DRM

G11C01622
Only 47 patents in class, none deal with DRM

H04L00900
H04L00930
H04L00932
When searching for (right*1 ADJ management) or ((copy OR copyright) ADJ protection) these classes together render the same results as H04L009

H04L01214
No DRM patents in H04L012 that are not in H04L01214 as well

H04L02906
H04L029 same results when searching (right*1 management) as H04L02906

H04N00716
Search using H04N00716 and H04N00716* and H04N00717*

H04N00703
No DRM patents in this class

H04N00724
H04N007 covers patents not in H04N00724

H04N005913
Searching H04N005 returns too many irrelevant results

Query classes (IPC):
G06F00100 OR G06F00946 OR G06F01214 OR G06F017 OR G11B00390 OR G11B02000 OR H04L00900 OR H04L00930 OR H04L00932 OR H04L01214 OR H04L02906 OR H04N007 OR H04N005913

Query classes (ECLA) - Questel Orbit format:

FILE PLUSPAT
/EC G06F-001/00N7R1
/EC G06F-001/00N7R2
/EC G06F-001/00N7A
/EC G06F-001/00N5A
/EC G06F-001/00N5A2
/EC G06F-001/00N5A2B
/EC G06F-001/00N5A2C
/EC G06F-001/00N5A2D
/EC G06F-001/00N5A2D2
/EC G06F-001/00N5A2T
/EC G06F-001/00N5P
/EC G06F-009/46R4
/EC G06F-012/14
/EC G06F-012/14B
/EC G06F-017/60
/EC G06F-017/60B

/EC G06F-017/60B8
/EC G11B-003/90
/EC G11B-020/00P
/EC G11B-023/28
/EC G11C-016/22
/EC H04L-009/00
/EC H04L-009/30
/EC H04L-009/32
/EC H04L-012/14
/EC H04N-007/16
/EC H04N-007/16D
/EC H04N-007/16E
/EC H04N-007/16E2
/EC H04N-007/16E2B
/EC H04N-007/16E3
/EC H04N-007/16F
/EC H04N-007/167
/EC H04N-007/167D
/EC H04N-007/169
/EC H04N-007/169B
/EC H04N-007/169C
/EC H04N-007/171
/EC H04N-007/171B
/EC H04N-007/171C
/EC H04N-007/173
/EC H04N-007/173B
/EC H04N-007/173B2
/EC H04N-007/173B3
/EC H04N-007/173B4
/EC H04N-007/173C
/EC H04N-007/173C2
/EC H04N-007/173C3
/EC H04N-007/03
/EC H04N-007/24C12P
/EC H04N-005/913

THIS PAGE INTENTIONALLY LEFT BLANK

This appendix contains all the patent numbers retrieved through the search in chapter 4 of the companies that were selected for review in chapter 5. After a manual review of each patent some are determined not to be DRM patents. All patents that do qualify as DRM patents according to the definition in chapter 3 have been classified according to the classification scheme presented in chapter 3 and have been summarized. As it is impossible due to time constraints to completely read every patent, the review has been limited to the summary and the principal claims.

Accenture or Anderson Consulting

1. WO0152095A2 *
2. WO0146846A2 *
3. WO2002077875A2 *
4. WO0139086A2 *
5. WO0139030A2 *

1,2,4,5 – Asset management in e-commerce focused on financial aspects; patents have very little or nothing to do with DRM in consumer electronics *-4.x-*

3 – Processing data (including assigning usage rights) in logical networks (i.e. data distributed over multiple physical networks) *-3.4-*

Canon

1. JP2001333405A *
2. EP1079627A1 *
3. EP0969668A2 *
4. US20020133705A1 *
5. US20020104003A1 *

1,2,3 – Using digital watermarking in MPEG-4 *-1.2.1-*

4, 5 – Watermarking apparatus and content distribution system or aspects thereof *-4.4.1-*

ContentGuard or Xerox

1. EP1146411A1 *
2. EP1146715A1 *
3. EP1146714A1 *
4. EP1113617A2 *
5. US20020108050A1 *
6. EP1130843A2 *
7. US6236971B1 *
8. US6330549B1 *
9. EP0999488A2 *
10. EP0715244A1 *
11. US5638443A1 *
12. US5634012A1 *
13. US5530235A1 *
14. US5629980A1 *
15. US5715403A1 *
16. EP1111838A2 *

1,9 – (Self-protecting documents) using polarization for protection *-1.1-*

2 – Content access protection using a blind transformation function -*1.1*-
3 – Content access protection using an additive encryption scheme -*1.1*-
4,6,16 – Changing decryption keys (a proxy encryption scheme) -*2 3*-
5 – Using a standard rendering engine in a DRM system -*2.4*-
7 – DRM architecture using tickets -*4.4.2*-
8 – Self-checking 'keep-alive' software -*1.1 / 2.5*-
10 – Controlling distribution based on a usage-rights grammar -*3.4*-
11 – DRM system for composite works -*4.4*-
12 – Fee accounting mechanism in DRM system -*3.2 / 4.x*-
13 – DocuCard system ("portable DRM system" – content depository) -*4.4*-
14 – DRM architecture in general based on usage rights -*4.4*-
15 – Usage rights grammar in DRM system (- most ContentGuard patents refer to a usage rights grammar in DRM systems) -*3 1*-

DigiMarc

1. WO2002086803A1 *
2. WO0250760A1 *
3. WO0195239A2 *

1 – DRM architecture based on content identification through watermarking -*4.4 / 1 2 1*-
2 – Architecture of watermark system in DRM/e-commerce systems -*4.4.1*-
3 – Watermark detection method (based on segmenting data) -*4.x*-

Hitachi

1 JP2002247342A
2. JP2000020587A
3. JP10232878A
4. JP10111833A
5 JP07084852A
6. JP04344955A
7. EP0977438A2
8. US20020116632A1

1 – Method of embedding copy control information in content using watermarks -*1.4*-
2 – DRM payment architecture -*4.4*-
3,4,5 – Access control architecture (focused on document access) -*4.4*-
6 – Setting temporary rights (using a table) -*3.1 / 3.2 / 3.4*-
7 – Compliancy management / device authentication -*2.2*-
8 – Architecture of a trusted computer system -*4.4*-

IBM

1. US6141754A1 *
2. US6418421B1 *
3. US6282653B1 *
4. EP1043672A2 *
5. US5673316A1 *
6. US20020147906A1 *
7. US20020095384A1 *
8. US20020091930A1 -unavailable
9. EP1191422A2 *
10. EP1001625A2 *
11. WO0111623A1 *

1 – End-to-end DRM system covering access control and rights management *-4.4-*
2 – Tracking usage of content on user devices *-4.2-*
3 – Royalty collection method *-3.2 / 4.x-*
4 – Secure content delivery system (using a RF receiver) *-1.1-*
5 – Cryptographic envelope (IBM's Cryptolope) *-1.1 / 4.4-*
6 – Key revocation *-2.5-*
7 – Content insurance (protecting rights from loss) *-3.3-*
9 – DRM system transparent to application layer on host system *-2.4 / 4.4-*
10 – Recording and playback control based on additional information embedded in the content – where the detector (for the embedded information) is not located in the drive *-4.4-*
11 – Copy management system *-4.4-*

Intel

1. US6389537B1
2. WO0129660A1
3. US5949877A1
4. WO0051287A1
5. US5915018A1

1 – Payment authentication system *-3.2-*
2 – DRM system (software player on disk) *-4.4-*
3,4 – Securely transferring content between devices (using certificates) *-2.3.4-*
5 – Key management between optical drive and content decompressor *-2.3-*

InterTrust

1. US5892900A1 *
2. WO0110076A2 *
3. US6138119A1 *
4. WO0109702A2 *
5. WO0106374A2 *
6. US6449367B2 *
7. WO0075925A1 *
8. US20020048369A1 *
9. US6427140B1 *
10. US6112181A1 *
11. WO9948296A1 *
12. WO0122320A2 *

1,8,9,10 – General DRM patents (cover general DRM architectures) *-these cover multiple classes-*
2 – Securing a trusted environment *-2.2-*
3 – Rights management data structures (important for example for interoperability) *-3.1-*
4 – Transaction protocols in DRM (including peer-to-peer) *-3.2 / 3.3 / 4.5-*
5 – Secure storage in a DRM system based on using a little secure storage to generate secrecy for a lot of insecure storage *-1.1-*
6 – Transmitting rights using watermarks *-3.3.1-*
7 – Content authentication using 2 watermarks (weak/strong) *-1.2.1-*
11 – DRM for streaming media *-4.4-*
12 – Auction model for selling content *-4.5-*

Macrovision

1. WO0051348A2
2. WO9641468A1
3. WO0141433A1
4. US6374036B1

1, 4 – Copy control system using watermarks *-1.4.1-*
2 – Copy control system using fingerprints and signatures *-1.4.3 / 1.4.4-*
3 – Circumvention method for copy protection systems based on video tag signals *-4.1-*

Matsushita

1. JP2002026835A *
2 JP2001312570A *
3. JP2000236435A *
4. US5987607A1 *
5. WO0062292A1 *
6. WO0116821A2 *
7. WO0067257A2 *
8. WO0028539A1 *
9. WO0225645A2 *
10. EP1158514A1 – as WO0052691
11 WO2002086685A2 *
12. WO2002071752A1 *
13 WO0161600A1 *
14 WO0021087A2 *
15. EP1098311A1 *
16. WO0195206A1 *
17. EP1018733A1 *

1 – Separate transmission of content en rights/keys *-3.2 / 3.3-*
2 – Detecting / identifying illegal copies of content *-1.2-*
3,10 – Copy control using watermark *-1.4 1-*
4 – Copy control system using ID's *-1.4-*
5 – DRM architecture for circulation content *-4.4-*
6 – DRM architecture with check-out to transfer content to portable memory card *-4.4 / 1.3-*
7 – Optical disk with 'key-block' *-1 1-*
8,14 – Superdistribution system (distribution system coupled to charging system) *-4.4-*
9 – Pit-sequence in optical disk to prevent copying *-1.1 6-*
11 – DRM architecture with separate management, relay and terminal device (enhances interoperability – specifically between different version of same DRM system) *-4.4 / 2.4-*
12 – IPMP standard for MPEG (info in content and tool in decoder) *-3.1-*
13 – Memory card with key-block *-1 1-*
15 – Revocation method *-2.5-*
16 – Creating rights management information based on licenses *-3.1 / 3.4-*
17 – DRM architecture using several decryption and encryption units *-4.4-*

Microsoft

1. US20020013772A1 *
2. US5999622A1 *
3. WO0201335A2 *
4. WO0201330A2 *
5. WO0201329A2 *
6. WO0169354A2 *
7. WO0146783A2 *
8. WO0115162A2 *
9 WO0201326A2 *
10. WO0106755A2 *
11. WO0152471A1 *
12. WO0146782A2 *

1 – Binding a license to a device *-2.2 / 1.4-*
2 – Method allowing partial encryption of a data file to enhance access speed *-4.x-*
3 – DRM architecture (focused on content rendering client) *-4.4-*
4, 5 – DRM architecture (focused on serving content) *-4.4-*
6 – Individualizing encryption (to prevent Break Once Run Everywhere, BORE) *-1.1 / 2.3-*
7 – DRM architecture *-4.4-*
8 – Identifying illegal copies *-4.2-*
9 – DRM architecture *-4.4-*
10 – Watermarking method (embeds signature) *-1.1 / 1.2-*
11 – DRM device deployment (initial key distribution) *-2.1-*
12 – Pre-releasing digital content by managing key distribution *-1.1 / 2.3 / 4.5-*

Philips

1. WO0173527A2 *
2. US20020023219A1 *
3. US20020078027A1 *
4. WO0159549A2 *
5. WO0142886A2 *
6. WO0152234A1 *
7. WO0067256A1 *
8. WO0058962A1 *
9. WO0068800A2 *
10. WO0004549A2 *
11. WO0028398A1 *
12. WO0104727A1 *
13. WO0021085A1 *
14. US20020152172A1 *
15. WO0159705A2 *
16. WO0157869A2 *
17. WO0156026A2 *
18. WO0064157A1 *
19. WO0004712A1 *
20. WO0105150A1 *
21. US20020120847A1 *
22. WO2002073378A2 *
23. WO2002065256A2 *
24. WO0231630A2 *
25. WO0157701A2 *
26. US20020144133A1 *
27. US20020076048A1 *
28. US20020073317A1 *
29. US6314518B1 *
30. US6473560B1 *

1 – Revocation list management (using a hierarchical "trust tree") -2.5-
2 – Protection against "copy and restore" attack (for embedded licenses) -3.4-
3 – Super distribution architecture -4.4-
4 – Content distribution method (the content provider's identifying information is stored in a central server) -4.4.4-
5,24 – Revocation list management (using a list of devices with which a device has communicated) -2.5-
6 – Securely transferring content between devices (by binding content to these devices in a sequential fashion) -2.3 / 1.4-
7 – Check-in / check-out system for DRM compliant devices -4.4 / 2.3-
8 – DRM architecture (using tickets) -4.4.2-
9 – Method to force updates of content screening system (software) in devices -2.1-
10 – Encryption scheme for content transfer between devices (using tickets) -2.3.2-
11 – DRM architecture (rights management is performed by software in which the content is encapsulated) -4.4-
12 – Method to process certificates in one-way communications (e.g. between decoder and display) -2.2-
13 – Copy control systems based on repositioning format information (e.g. writing the FAT table to a different location on a disk) -4.x-
14,26 – Content screening circumvention technology -4.1 / 1.2-
15,16,17,28 – Complete data set technology (e.g. all tracks on CD must be present) -1.2.9-
18,20 – Secure method of transferring content between devices -2.3-
19 – Copy control system using watermarks, tickets and one-way hashes -1.2-
21 – Secure transfer of content between (trusted) devices and method of authenticating these devices -2.2 / 2.3-
22 – Binding content to a group of devices (and managing expansion and such of this group of devices) -1.4 / 2.2 / 2.3-
23 – Processing copy protection signals (e.g. watermarks) -3.4-
25 – DRM business method implementation ("buy-button" on device) -4.5-
27 – Protection against splitting and afterwards merging protected content to circumvent copy protection schemes -1.2-
29 – Transferring rights management information between devices -3.3 / 2.3-
30 – "Translating" a digital ticket to an analog one -3.4 / 1.4 / 2.4-

SealedMedia

1. GB2367925A *
2. GB2367668A *
3. WO0231648A2 *
4. WO0231632A2 *
5. WO0195175A2 *

1 – Attaching rights to a mobile device that can be attached to a consumer device -1.4 / 2.2-
2 – Search engine for encrypted content -4.x-
3 – Using encryption to make a trusted JAVA-environment -2.x-
4 – Patching an OS to make it trusted -2.x-
5 – DRM architecture (rights stored on server) -4.4 / 3.2-

Sony

1. JP11177924A *
2. JP2002215465A - as WO2002056535A1
3. JP2001118332A *
4. JP2001005732A *
5. EP1054314A2 *
6. EP1058257A1 *
7. EP1067469A2 *
8. EP0901124A2 *
9. EP0942417A2 *
10. EP1128598A1 *
11. EP1014361A2 *
12. EP1079624A2 *
13. EP1005040A1 *
14. EP1069773A2 *
15. US20020085311A1 *
16. US6266482B1 *
17. US20020006199A1 *
18. US6480607B1 *
19. EP1253739A1 *
20. EP1253738A1 *
21. EP1249962A1 *
22. EP1134670A1 *
23. EP1120715A1 *
24. US6363149B1 *
25. EP0899733B1 *

1 – Watermarking for copy protection (in analogue signal) *-1.3-*
2 – Separate trusted circuit in reading/writing device for recordable key-block 4.x
3 – DRM architecture (focused on transaction protocols) *-4.4-*
4 – Copy control system (for stream) *-4.4-*
5 – Key management in terminal *-2.3-*
6, 11 – Copy control limiting copies of first generation content (original) *-4.4-*
7 – Business method (price differentiation based on usage volume) *-4.5-*
8 – Watermarking method (embedding copy control info) *-1.4-*
9,23 – DRM architecture (payment method) *-4.4-*
10, 22 – DRM architecture/system *-4.4-*
12 – Data/copy control information storage system *-3.4-*
13 – Copy control information embedding method/system allowing detection in both compressed and uncompressed state of content *-1.4-*
14 – Copy control information embedding method/system using multiple streams (e.g. audio/video) *-1.4-*
15 – Method of determining copy protection features and displaying these to the user *-3.4 / 4.x-*
16 – Method of embedding copy protection information in video *-1.4-*
17 – Copy control system (bridging digital to analogue) *-1.3-*
18 – Copy control system using two watermarks (separate audio/video) *-1.4.1-*
19,20,21 – Key management (using a tree structure) *-2.3-*
24 – Key management (deriving previous keys through hash functions) *-2.3-*
25 – Optical disk copy protection (key-block) *-1.1.8-*

Thomson

1. WO9828913A2 *
2. WO9728630A2 *
3. WO2002084996A1 *
4. WO2002078341A2 *
5. WO2002054196A2 *
6. WO0175876A1 *

1,6 – Copy control system *-4.4-*
2 – Method of (securely) sharing information (e.g. password) between consumer devices *-2.3-*
3 – Encryption of content over Firewire *-2.3-*
4 – Encryption system for transferring content between devices *-2.3-*
5 – Superdistribution architecture *-4.4-*

Toshiba

1. US6438692B1
2. EP0908881A2
3. EP1182825A2

1 – Copy control using a disk key (embedded/watermark) *-1.1.1-*
2 – Copy control using a watermark (in ECC) on an optical disk *-1.1.1-*
3 – Secure content transfer (using radio link layer) *-1.1 / 3.1-*

The classification of the patents in each company's portfolio can be summarized. The tables below indicate:

- The number of patents in class 1.1 / 1.2 / 1 (excluding 1.1 and 1.2) / total in class 1
- The number of patents in class 2
- The number of patents in class 3
- The enabling technology most frequently used in patents (if any) or a comment on the portfolio

Class 4 is left out, as the patents in this class are too diverse to make a comparison. As some patents have been assigned multiple classes, these tables do not show the total number of patents for each class. However, they do give an indication of the strength of a companies DRM portfolio in the three classes of DRM technologies.

Canon

Class 1	Class 2	Class 3	Technology
0/3/0/3	2	0	Watermarking

ContentGuard

Class 1	Class 2	Class 3	Comment
1/0/0/1	5	3	Rights grammars

DigiMarc

Class 1	Class 2	Class 3	Technology
0/1/0/1	0	0	Watermarking

Hitachi

Class 1	Class 2	Class 3	Technology
0/0/1/1	1	3	

IBM

Class 1	Class 2	Class 3	Technology
1/0/0/1	2	2	

Intel

Class 1	Class 2	Class 3	Technology
0/0/0/0	3	1	

InterTrust

Class 1	Class 2	Class 3	Comment
1/0/0/1	1	4	Several patents cover DRM in general

Macrovision

Class 1	Class 2	Class 3	Technology
0/0/4/4	0	0	Large variety in technologies used

Matsushita

Class 1	Class 2	Class 3	Technology
3/1/4/8	2	4	

Microsoft

Class 1	Class 2	Class 3	Technology
3/1/1/5	4	0	

Philips

Class 1	Class 2	Class 3	Technology
0/6/3/9	17	3	Complete data set (which uses watermarking, tickets and such)

SealedMedia

Class 1	Class 2	Class 3	Technology
0/0/1/1	3	1	

Sony

Class 1	Class 2	Class 3	Technology
1/0/6/7	5	2	

Thomson

Class 1	Class 2	Class 3	Technology
0/0/0/0	3	0	

Toshiba

Class 1	Class 2	Class 3	Technology
3/0/0/3	0	1	Watermarking

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix D - Searching for Philips' DRM Patents

The patents in the Philips DRM patent list contain equivalents, which means that one patent can appear on the list multiple times (e.g. the same patent listed once as a WO application and once as a EP patent). It is possible to have the patent databases that are used, automatically remove equivalents from the results. This can result however, in patents being removed that stem from the same application, but are essentially different. An example of when this can happen is when a single patent application has been split into two different applications, because the patent essentially covers two different inventions. In that case both patents stem from the same application and will therefore be seen as family meaning one of them will be removed from the results.

As the list of Philips patents needs to be as complete as possible, equivalents will not be removed automatically. All these patents will be reviewed manually and it is possible at the time of manual review to remove patents that are listed twice.

Figure 4.9 (see below) shows the intermediate results of the process of determining which DRM patents Philips holds. The results of Query 3 are split into two groups: one group of patents with an ECLA and one group of patents without an ECLA. The first group is filtered using the ECLA classification the second group is filtered using the IPC classification. As all patents are manually reviewed, it is possible to determine if the filtering using IPC and ECLA has returned correct results. This is indicated in the graph as the false positive and false negative rate. The false negative rate indicates the percentage of patents that were wrongfully filtered out of the results based on IPC or ECLA. The false positive rate indicates the percentage of patents that should have been filtered out but weren't.

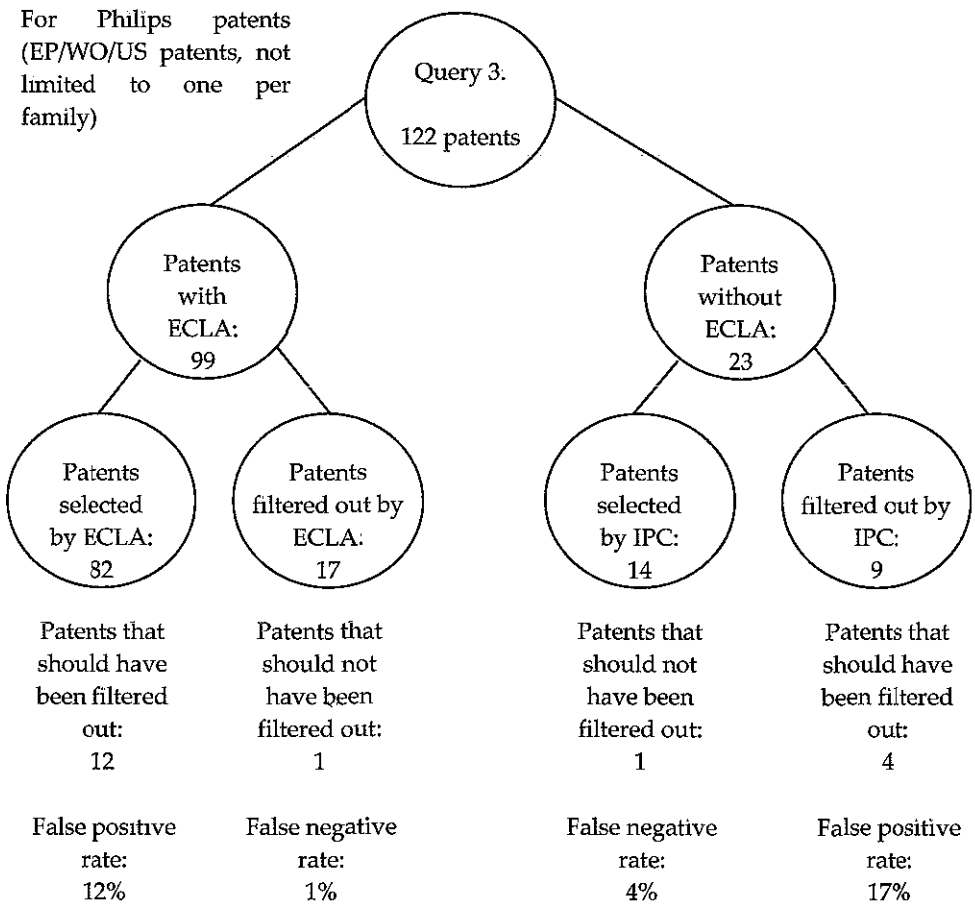


Figure 4.9: Results of Query 3 and filtering for Philips DRM patents

It is clear that filtering using ECLA is characterized by lower, hence better, false positive and false negative rates[75].

[75] If all the patents were filtered using IPC, the false negative and false positive rates would also be higher than they are for filtering using the ECLA.

Developi

Philips' Digital Rights Management Patent Portfolio

Patents are an important business tool. There is a need for companies to plan their patent operations, through the use of a patent strategy. Such a strategy aids a company in strengthening its position amongst other patent holders. In this case study, a strategy is determined for Philips' portfolio of patents on Digital Rights Management (DRM) technologies. Such technologies manage the interaction with digital content.

In order to determine the patent strategy, a search is conducted for DRM patents. The patent holders and their patents are then compared. The results of this comparison as well as patent strategy theory and a strategy choice decision model are used to determine which strategy Philips should follow.